HOCHSCHULE FÜR ÖFFENTLICHE

VERWALTUNG UND FINANZEN LUDWIGSBURG

Das neuseeländische Konzept RealMe zur elektronischen Identifizierung – Ein möglicher Ansatz für die deutsche Verwaltung?

BACHELORTHESIS

zur Erlangung des Grades eines

Bachelor of Arts (B.A.)

im Studiengang gehobener Verwaltungsdienst – Public Management

vorgelegt von

Lea Denise Miene

Studienjahr 2015 / 2016

Erstgutachter: Prof. Dr. Robert Müller-Török

Zweitgutachter: Mag. Peter Kustor

Inhaltsverzeichnis

Abkürzungsverzeichnis ..... **V**

Glossar ..... **VII**

Abbildungsverzeichnis ..... **VIII**

Anlagenverzeichnis ..... **IX**

1 Einleitung **1**

2 Die Notwendigkeit der physischen Anwesenheit beim Erledigen behördlicher Vorgänge in Deutschland **4**

3 Benutzung von Ausweisdokumenten in Deutschland **6**

3.1 Allgemeine Informationen und rechtliche Grundlagen 6

3.2 Elektronische Ausweisdokumente 7

4 Der neue Personalausweis **9**

4.1 Die unterschiedlichen Funktionen 9

4.1.1 Biometrie-Funktion 9

4.1.2 eID-Funktion 9

4.1.3 Unterschriftsfunktion 10

4.2 Rechtliche Rahmenbedingungen für die eID-Funktion 11

4.3 Voraussetzungen für die Nutzung 11

4.3.1 Was benötigt der Nutzer? 12

4.3.2 Was benötigt der Dienstanbieter? 13

4.4 Ablauf der Online-Identifikation mit dem nPA 14

4.5 Vor- und Nachteile der eID-Funktion des nPA 15

4.6 Mögliche Anwendungsbereiche und zugelassene Dienstanbieter 16

4.7 Datenschutz- und Datensicherheit 17

4.8 Probleme und Hindernisse bei der Nutzung 18

5 Benutzung von Ausweisdokumenten in Neuseeland 20
5.1 Allgemeine Informationen und rechtliche Grundlagen 20
5.2 Elektronische Identifikation 21
6 Das neuseeländische Konzept RealMe 23
6.1 Allgemeine Informationen 23
6.1.1 Entstehung und Hintergründe 24
6.1.2 Rechtliche Rahmenbedingungen 24
6.2 Die unterschiedlichen RealMe Benutzerkonten 25
6.2.1 Das nicht verifizierte RealMe Benutzerkonto 25
6.2.2 Das verifizierte RealMe Benutzerkonto 26
6.2.2.1 Verifizieren des Benutzerkontos 27
6.2.2.2 Was benötigt der Nutzer? 28
6.2.2.3 Der Ablauf einer Online-Identifikation mit RealMe 29
6.2.2.4 Second-Factor-Authentication 30
6.2.3 Die verifizierte Adresse 31
6.2.4 Die elektronische Signatur bei RealMe 31
6.2.5 Mögliche Anwendungsbereiche 32
6.3 RealMe für Dienstanbieter 33
6.4 Nutzung von RealMe im Vergleich zur physischen Identifikation 34
6.4.1 RealMe im Vergleich zum nPA 35
6.4.2 Vorteile durch die Nutzung von RealMe 36
6.4.3 Nutzungsauswertung anhand von Statistiken 36
6.5 Datenschutz und Sicherheit 38
7 Ein mögliches RealMe-Konzept für Deutschland 39
7.1 Rechtliche Umsetzung 40
7.1.1 Problematik durch rechtliche Rahmenbedingungen 40
7.2 Technische Umsetzung 43

7.3 Organisatorische Umsetzung 43
7.3.1 Zu beteiligende Institutionen 44
7.3.2 Infrastruktur 45
7.3.3 Voraussetzungen 45
7.3.4 Möglichkeiten zur Förderung von Online-Diensten 46
7.4 Vor- und Nachteile beim Anbieten eines solchen Dienstes 48
7.5 Problematik 49
8 Mögliche Weiterentwicklung der Thematik 51
9 Fazit 53

Literaturverzeichnis 55
Eidesstattliche Erklärung 61

Abkürzungsverzeichnis

Abs.	Absatz
AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism Act
BDSG	Bundesdatenschutzgesetz
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
DIA	Department of Internal Affairs
eAT	elektronische Aufenthaltstitel
e-GIF	e-Government Interoperability Framework
EGovG	E-Government-Gesetz
eID	elektronische Identität
eiDAS-VO	Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
EIV	Electronic Identity Verification
ELSTER	Elektronische Steuererklärung
EOI	Evidence of Identity
ePass	elektronischer Pass
EU	Europäische Union
GG	Grundgesetz
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
KfZ	Kraftfahrzeug

nPA	neuer Personalausweis
NZ Post	New Zealand Post
PAuswG	Personalausweisgesetz
PAuswV	Personalausweisverordnung
PIN	Persönliche Identifikationsnummer
PUK	Personal Unblocking Key
QES	qualifizierte elektronische Signatur
SAML	Security Assertion Markup Language
STORK	Secure Identity Across Borders Linked
TAN	Transaktionsnummer
VO	Verordnung
VwVfG	Verwaltungsverfahrensgesetz

Glossar

E-Government

Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten mithilfe von Informations- und Kommunikationstechniken über elektronische Medien.[1]

Digital Natives

Die erste Generation, die mit dem Internet aufwächst.[2]

Implementieren

Das Einsetzen von Software in ein bestehendes Computersystem um dadurch ein funktionsfähiges Programm zu erstellen.[3]

Interoperabilität

Beschreibt die Fähigkeit unterschiedlicher Systeme möglichst nahtlos zusammenzuarbeiten.[4]

Medienbruchfrei

Medienbruchfrei ist ein Ablauf dann, wenn bei der Übertragung von Informationen kein Wechsel des Mediums erfolgt, also z.B. kein Wechsel von PC zu Papier, sondern der ganze Prozess über ein Medium erfolgt.

Mobiles Endgerät

Geräte, die ohne weiteren Aufwand mitgenommen und von unterwegs genutzt werden können, z.B.: Smartphone, Tablet, Notebook.

Section

---

[1] Gabler Wirtschaftslexikon: E-Government, URL: http://wirtschaftslexikon.gabler.de/Definition/electronic-government.html?referenceKeywordName=E-Government (aufgerufen am 28.08.2015).
[2] Vgl. Habbel, Franz-Reinhard, S.451.
[3] Duden: Implementierung, URL: http://www.duden.de/rechtschreibung/implementieren (aufgerufen am 31.08.2015).
[4] Duden: Interoperabilität, URL: http://www.duden.de/rechtschreibung/Interoperabilitaet (aufgerufen am 31.08.2015).

Abschnitt in englischsprachigen (hier: neuseeländischen) Gesetzen und Verordnungen.

Verifizieren

Die Richtigkeit einer Sache durch Überprüfen bestätigen.[5]

Abbildungsverzeichnis

Abbildung 1: Dienstanbieter werden.....14
Abbildung 2: Ablauf der Online-Identifikation mit dem nPA.....15

[5] Duden: verifizieren, URL: http://www.duden.de/rechtschreibung/verifizieren (aufgerufen am 07.09.2015).

Abbildung 3: Benötigte Nachweise und Nutzungszahlen des verifizierten Benutzerkontos 28
Abbildung 4: Ablauf der Online-Identifikation mit RealMe 29
Abbildung 5: Erstanmeldungen und Wiederbenutzung 37
Abbildung 6: Anstieg der verifizierten Benutzerkonten 38

Anlagenverzeichnis

-Alle Anlagen befinden sich auf der beigefügten CD-

Kapitel 1:

Anlage 1.1 Cartoon Peter Steiner

Anlage 1.2 E-Mail des BMI vom 30.07.2015

Anlage 1.3 Leitfaden Online-Ausweisfunktion

Kapitel 2:

Anlage 2.1 Minikommentar zum EGovG

Anlage 2.2 Leitfaden Online-Ausweisfunktion (siehe Anlage 1.3)

Kapitel 3:

Anlage 3.1 Leitfaden Online Ausweisfunktion (siehe Anlage 1.3)

Anlage 3.2 E-Mail des BMI vom 30.07.2015 (siehe Anlage 1.1)

Kapitel 4:

Anlage 4.1 Personalausweisbroschüre

Anlage 4.2 Certificate Policy

Anlage 4.3 E-Mail des BSI vom 22.06.2015

Anlage 4.4 Leitfaden Online-Ausweisfunktion (siehe Anlage 1.3)

Anlage 4.5 Flyer Bundesdruckerei Sicherheitsmerkmale

Kapitel 5:

Anlage 5.1 Document Verification Guide

Anlage 5.2 E-Mail des Business Support Officer vom 19.08.2015

Kapitel 6:

Anlage 6.1 About RealMe

Kapitel 7:

Anlage 7.1 Certificate Policy (siehe Anlage 4.2)

Anlage 7.2 Minikommentar zum EGovG (siehe Anlage 2.1)

Anlage 7.3 Mobile Fokusgruppe BVDW

Kapitel 8:

Anlage 8.1 Minikommentar zum EGovG (siehe Anlage 2.1)

1 Einleitung

„ On the internet nobody knows you´re a dog.“[6]

Dieser aus einem Cartoon stammende Spruch verdeutlicht die Anonymität, die das Internet seinen Nutzern bieten kann. Anonymität ist in vielen Bereichen des Internets sehr wichtig und oftmals kann dort nicht nachvollzogen werden, mit wem man es gerade zu tun hat. „ Die Anonymität im Internet verleitet [daher] viele, die Unwahrheit über sich zu erzählen.“[7] Wer einem im Internet tatsächlich gegenübersitzt ist für Dienstanbieter oft nicht erkennbar und auch Internetnutzer haben oftmals keine Gewissheit ob der Dienstanbieter, mit dem sie eine Transaktion durchführen, auch wirklich dazu berechtigt ist und in dieser Form existiert.

Vor allem der Generation der Digital Natives, fällt es in manchen Situationen aber nahezu einfach, ihre persönlichen Daten, ihre Identität, preiszugeben. Richtig genutzt und gezielt eingesetzt kann die Freigabe persönlicher Daten im Internet vor allem für Dienstanbieter enorme Vorteile bringen. Vorausgesetzt der Dienstanbieter kann sich über die Richtigkeit der Daten sicher sein und diese liegen ihm so vor, dass er sie auch verarbeiten kann.

Geht es um offizielle Angelegenheiten, wie die Steuererklärung, die Beantragung eines Führungszeugnisses oder eines Kredits bei der Bank, muss auch für den Nutzer gesichert sein wer persönliche Daten in welchem Umfang einsehen kann und vor allem wofür sie genutzt werden dürfen. Sowohl Nutzer als auch Dienstanbieter benötigen eine Garantie darüber, wer ihr Gegenüber ist. Um auch über das Internet eine Kontrolle über die Freigabe von identitätsbezogenen Daten zu haben wurde daher

[6] Vgl. Anlage 1.1, Cartoon von Peter Steiner,
(erschienen in: ´The New Yorker´ am 05.07.1993).
Übersetzung: Im Internet weiß niemand, dass du ein Hund bist.
[7] Cole, Tim, S. 522.

2010 der neue Personalausweis, kurz nPA, mit der Funktion als eID eingeführt.[8]

Dennoch hat nur knapp über ein Viertel der Inhaber des neuen Personalausweises die Funktion des elektronischen Identitätsnachweises überhaupt freigeschaltet.[9]

Gerade in der Zeit der Digitalisierung könnten die Nutzung und das Angebot von Online-Dienstleistungen aber vieles vereinfachen und Bearbeitungs- und Wartezeiten verkürzen. Sowohl für die Bürger als auch für die Behörden könnte eine verstärkte Nutzung Vorteile bringen.

In dieser Bachelorthesis geht es darum die Möglichkeiten zu erkennen, die es gibt, um die elektronische Identifizierung gegenüber Behörden zu vereinfachen. Es soll dargestellt werden, wie die elektronische Identifizierung sinnvoll in Verwaltungs- und Geschäftsabläufe integriert werden kann. Gestützt wird die Beantwortung dieser Frage auf ein Konzept zur elektronischen Identifizierung aus Neuseeland, das dort den Gang zur digitalen Behörde ermöglicht und mit welchem Vorgänge medienbruchfrei und abschließend über das Internet erledigt werden können.

Das Ziel ist es herauszufinden, ob die neuseeländische Lösung zur Nutzung der elektronischen Identifizierung ein Ansatz für die deutsche Verwaltung zur verstärkten Nutzung solcher Dienste sein könnte, und ob diese Lösung in Deutschland umsetzbar wäre.

Methodisch ist diese Bachelorthesis wie folgt aufgebaut:
Zunächst wird die Notwendigkeit der physischen Anwesenheit beim Erledigen behördlicher Vorgänge in Deutschland erläutert und es wird ein Blick auf die Benutzung von Ausweisdokumenten in Deutschland geworfen. Danach wird die bisherige deutsche Lösung zur elektronischen Identifizierung, der neue Personalausweis, näher betrachtet. Anschließend

[8] Vgl. Anlage 1.3, Leitfaden Online-Ausweisfunktion in Behörden.
[9] Vgl. Anlage 1.1, E-Mail des BMI.

wird auf die Benutzung von Ausweisdokumenten in Neuseeland eingegangen und das neuseeländische Konzept RealMe zur elektronischen Identifizierung wird vorgestellt.
Danach soll aufgezeigt werden, ob ein solches Konzept auch Potenzial für die deutsche Verwaltung hätte und ob eine Umsetzung möglich wäre. Zum Ende wird thematisiert, wie eine mögliche Weiterentwicklung der elektronischen Identifikation aussehen könnte und was die gezielte Nutzung langfristig an Folgen und Auswirkungen auf unser Verwaltungshandeln und unseren Alltag haben könnte.

Abbildungen und Tabellen dienen zur Ergänzung dieser Bachelorthesis. Notwendige Übersetzungen wurden vom Autor vorgenommen. Die männliche Form gilt in dieser Bachelorthesis aus Gründen der Vereinfachung und der besseren Lesbarkeit für Personen beiderlei Geschlechts.

2 Die Notwendigkeit der physischen Anwesenheit beim Erledigen behördlicher Vorgänge in Deutschland

Der ursprüngliche Personalausweis diente hauptsächlich zur Identifikation einer Person Vor-Ort, beispielsweise zur Identifikation bei einer Polizeikontrolle oder bei der Beantragung eines Führerscheins. Der nPA versprach diese Notwendigkeit der physischen Anwesenheit beim Erledigen behördlicher Vorgänge zu reduzieren. Für behördliche Dienstleistungen ist aber in den meisten Fällen nach wie vor der Gang zum Amt unerlässlich.

Etwas im Bereich der Verwaltung abschließend von zuhause oder unterwegs zu erledigen ist beinahe unmöglich. Es gibt nur wenige gut funktionierende Beispiele von Behörden, bei denen Dinge abschließend erledigt werden können ohne persönlich zur Behörde gehen zu müssen. Meistens kann man sich lediglich informieren.[10] Allgemein werden aber immer mehr Aktivitäten aus unserem Alltag ins Internet verlagert,[11] weshalb es an der Zeit ist, dass auch im Bereich der Verwaltung mehr Möglichkeiten zur Nutzung des digitalen Umfelds geschaffen werden.

Immerhin bieten viele Behörden bereits ihre Vordrucke und Antragsformulare im Internet an. Auch das Onlineportal ´service-bw´[12], welches in Baden-Württemberg versucht behördenübergreifend Dokumente und Formulare online anzubieten ist ein guter Ansatz zur Vereinfachung der Verwaltung.

Anträge für die eine Identifikation der Person vorgeschrieben ist, lassen sich online noch fast nirgendwo abschließend abwickeln. Auch Anträge für die kein Identitätsnachweis gefordert wird, wie beispielsweise Anträge für das An- oder Abmelden von Mülltonnen, stehen in den meisten Fällen nur als Formular zum Download bereit. Dieses Formular muss allerdings in Ermangelung der rechtskräftigen Unterschrift ausgedruckt und dann unterschrieben zur Behörde gebracht werden, um dort weiter bearbeitet

[10] Vgl. Anlage 2.1, Minikommentar EGovG, S.3.
[11] Vgl. Anlage 2.2 Leitfaden Online-Ausweisfunktion in Behörden.
[12] Für weitere Informationen siehe: https://www.service-bw.de/.

werden zu können.[13] Auch hierfür bietet der nPA grundsätzlich eine Möglichkeit den Papierkrieg zu umgehen und das Dokument mittels elektronischer Signatur zu unterzeichnen.

Es gibt aber auch ein gutes Beispiel für die abschließende Erledigung von Dienstleistungen in der Verwaltung. Das Programm ´ELSTER´[14] bietet die Möglichkeit ohne ein Dokument ausdrucken zu müssen die eigene Lohnsteuererklärung von zuhause aus zu bearbeiten und an das zuständige Finanzamt zu versenden, oder die eigene Lohnsteuerkarte einzusehen.

Im Verwaltungsdschungel in Deutschland ist allerdings weitaus mehr Einsatz elektronischer Möglichkeiten nötig um tatsächlich Abhilfe zu schaffen und sowohl die Verwaltung zu entlasten als auch für den Bürger die Verwaltung zugänglicher und attraktiver zu machen. Dabei wird der Einsatz von E-Government zukünftig auch vermehrt ein Standortfaktor und bestimmt die Wettbewerbsfähigkeit.[15]

[13] Vgl. Anlage 2.1, Minikommentar EGovG, S.3.
[14] Für mehr Informationen siehe: https://www.elster.de/.
[15] Vgl. Stingl, Johannes, S. 124.

3 Benutzung von Ausweisdokumenten in Deutschland

In diesem Kapitel werden zunächst die Grundlagen für die Benutzung von Ausweisdokumenten in Deutschland erläutert und es wird dargestellt welche Dokumente in Deutschland als Ausweisdokumente anerkannt werden. Das Hauptaugenmerk soll auf der Benutzung von elektronischen Ausweisdokumenten liegen.

3.1 Allgemeine Informationen und rechtliche Grundlagen

Ein Ausweis ist ein von offizieller staatlicher Stelle ausgestellter Identitätsnachweis, welcher nach einem einheitlichen Muster[16] auszustellen ist. Der Ausweis stellt bestimmte rechtliche Eigenschaften einer Person, zum Beispiel die Staatsangehörigkeit, dar und gibt weitere Attribute, wie beispielsweise die Augenfarbe und Größe, an. Der Besitz eines gültigen Ausweisdokumentes ist für alle deutschen Bundesbürger Pflicht, sobald sie 16 Jahre alt sind.[17]

Es gibt unterschiedliche Personenkreise für die jeweils ein anderes Dokument, basierend auf unterschiedlichen Rechtsgrundlagen, in Deutschland die Wirkung eines Ausweisdokumentes hat. Ein Personenkreis sind Personen mit deutscher Staatsangehörigkeit. Für sie regelt § 2 Absatz 1 PAuswG welche Dokumente innerhalb Deutschlands als Ausweis gelten: „Ausweise im Sinne dieses Gesetzes sind der Personalausweis und der vorläufige Personalausweis“. Eine Pflicht zur Mitführung des Personalausweises gibt es nicht, lediglich die Pflicht zum Besitz.[18] Auf Verlangen muss der Personalausweis jedoch zur Identitätsfeststellung der berechtigten Behörde vorlegt werden.[19]

Ein anderer Personenkreis umfasst die Personen, die aus Nicht-EU-Ländern stammen, und unter das Aufenthaltsgesetz fallen. Für diese Drittstaatenangehörige ist ein Aufenthaltstitel erforderlich.[20] Dieser wird

[16] Siehe § 5 Abs. 1 PAuswG.
[17] Siehe § 1 Abs. 1 S.1 PAuswG.
[18] Siehe § 1 Abs. 1 S.1 PAuswG.
[19] Siehe § 1 Abs. 1 S.2 PAuswG.
[20] Siehe § 4 AufenthG.

auch mit der Funktion als eID ausgestellt. Für Ausländer, Asylsuchende und Flüchtlinge gibt es außerdem den elektronischen Reiseausweis.[21]

3.2 Elektronische Ausweisdokumente

Im November 2010 wurde der neue Personalausweis mit der Funktion als eID in Deutschland eingeführt, mit dem Hintergrund ein neues und sicheres Ausweisdokument zu schaffen.[22] Im Vergleich zu seinem Vorgänger gab es einige Änderungen beim neuen Personalausweis.[23] Das offensichtlichste ist, dass der Personalausweis seither Scheckkartengröße hat, was ihn deutlich handlicher macht. Die sichtbare Beschriftung enthält nun auch die Postleitzahl und das Personalausweislogo. Der neue Personalausweis verfügt über einen kontaktlos lesbaren Chip im Ausweis.[24] Außerdem verfügt er über eine Online-Ausweisfunktion und es besteht die Möglichkeit der Unterschriftsfunktion.

Das BMI gibt an, dass seit der Einführung im November 2010 bis Ende Juli 2015 etwa 31.000.000 neue Personalausweise produziert wurden.[25] Dieser Wert entspricht allerdings nicht der tatsächlichen Anzahl der Personen, die einen neuen Personalausweis besitzen, da zu diesem Wert auch Neuausstellungen aufgrund von Diebstahl, Verlust oder Namensänderung gezählt werden.[26] Bis zum Jahr 2020 werden alle ausweispflichtigen Deutschen ihren alten Personalausweis gegen den nPA eingetauscht haben.[27]

---

[21] Bundesministerium des Innern: elektronischer Reiseausweis, URL: http://www.bmi.bund.de/DE/Themen/Moderne-Verwaltung/Ausweise-Paesse/Dokumente-Auslaender/Elektronischer-Reiseausweis/elektronischer-reiseausweis_node.html (aufgerufen am 25.08.2015).

[22] Vgl. Imhof, Maximilian, S. 47.

[23] Personalausweisportal: Der Ausweis mit dem Klick, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/der-personalausweis_node.html (aufgerufen am 08.08.2015).

[24] Vgl. Anlage 3.1, Leitfaden Online Ausweisfunktion.

[25] Vgl. Anlage 3.2, E-Mail des BMI.

[26] Vgl. Anlage 3.2, E-Mail des BMI.

[27] Personalausweisportal: FAQ Dienstanbieter, URL: http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/FAQ/faq_node.html#faq3241822 (aufgerufen am 08.08.2015).

Zusätzlich zum neuen Personalausweis gibt es in Deutschland auch noch den ePass und den eAT als elektronische Ausweisdokumente.[28] EU-Bürger, die weder Deutsche im Sinne des Artikel 116 Abs. 1 GG noch Drittstaatenangehörige sind, werden in Deutschland von der Möglichkeit der elektronischen Identifikation ausgeschlossen. Anders herum ist es bisher aber auch nicht möglich „ nationale Mittel zur elektronischen Identifizierung, wie z.B. den deutschen Personalausweis mit elektronischer Identifizierungsfunktion auch in anderen Mitgliedsstaaten für die Kommunikation mit der öffentlichen Verwaltung einzusetzen.“[29] Die Möglichkeit zur EU-weiten elektronischen Identifizierung soll zukünftig durch die eiDAS-VO angepasst und besser geregelt werden.

Im nachfolgenden Kapitel 4 wird ausschließlich auf den nPA als elektronisches Ausweisdokument eingegangen.

[28] Bundesamt für Sicherheit in der Informationstechnik: Elektronische Ausweise, URL: https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/elektronischeausweise_node.html (aufgerufen am 08.08.2015).

[29] Sosna, Sabine, S. 825.

4 Der neue Personalausweis

In diesem Kapitel soll der nPA detailliert vorgestellt werden, um den aktuellen Stand der elektronischen Identifizierung in Deutschland darzustellen und aufzuzeigen, wo die Gründe für die geringen Nutzungszahlen liegen könnten.

4.1 Die unterschiedlichen Funktionen

Der nPA vereint drei unterschiedliche Funktionen, die nachfolgend vorgestellt und jeweils kurz erläutert werden. Die wichtigste Funktion im Rahmen dieser Bachelorthesis ist die eID-Funktion. Sie wird aus diesem Grund zuerst kurz vorgestellt und anschließend ausführlich behandelt. Dabei werden Funktionsweise und Anwendungsbereiche vorgestellt, sowie Vor- und Nachteile erläutert.

4.1.1 Biometrie-Funktion

Mit der Verabschiedung des Terrorismusbekämpfungsgesetzes im Jahr 2002 wurden zur Erhöhung der Sicherheit erstmals biometrische Merkmale in den Personalausweis aufgenommen. Artikel 8 Nr. 1a) dieses Gesetzes legt fest: „Der Personalausweis darf neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten.“ Die auf dem Chip des Personalausweises gespeicherten biometrischen Merkmale sind das Lichtbild, ein Teil der auf den Personalausweis aufgedruckten Informationen und gegebenenfalls die Fingerabdrücke.[30]

4.1.2 eID-Funktion

Mit der eID-Funktion des Personalausweises können personenbezogene Daten elektronisch übermittelt werden. Dadurch ist es auf der einen Seite dem Inhaber möglich seine Identität im Internet eindeutig nachzuweisen. Behörden und anderen Stellen ist es möglich ihr Gegenüber im

[30] Vgl. Anlage 4.1, Personalausweisbroschüre S.6.

elektronischen Rechts- und Geschäftsverkehr eindeutig zu identifizieren. Biometrische Daten werden mit der eID-Funktion nicht übermittelt.[31]

Die Zahl der neuen Personalausweise, bei denen die eID-Funktion aktiviert wurde, liegt laut Angaben des BSI bei knapp 30 %, was eine Anzahl von etwa 12 Millionen aktivierten Ausweisen ausmacht.[32] Verglichen mit der aktuellen Bevölkerungszahl in Deutschland von rund 81 Millionen Menschen[33] ist die Zahl der Personalausweise mit aktivierter eID sehr gering. Selbst dann, wenn die Zahl der Personen abgezogen wird, die keinen nPA besitzen oder für die eine Nutzung der eID-Funktion aus anderen Gründen nicht in Frage kommt.

4.1.3 Unterschriftsfunktion

Mit der Unterschriftsfunktion des neuen Personalausweises ist es möglich Dokumente, die digital vorliegen, rechtsverbindlich zu unterzeichnen.[34] Dazu wird eine qualifizierte elektronische Signatur (QES) benötigt. Zusätzlich ermöglicht die QES es, nachzuprüfen ob elektronisch signierte Dokumente nach dem digitalen Unterzeichnen nochmals verändert wurden.[35] Der nPA ist zwar für die Unterschriftsfunktion vorbereitet aber für die Nutzung muss ein zusätzliches Signaturzertifikat erworben werden.[36] Die Unterschriftsfunktion des nPA hat keine Verbindung zur eID-Funktion und ist als separate Funktion anzusehen.[37]

Für die Verwaltung ist die QES im Verwaltungsverfahrensgesetz (VwVfG) geregelt. § 3a Absatz 2 VwVfG legt fest: „ Eine durch Rechtsvorschrift angeordnete Schriftform kann, […], durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer

[31] Vgl. Anlage 4.2, Certificate Policy, Kapitel 1.1.
[32] Vgl. Anlage 4.3, E-Mail des BSI über Nutzungszahlen.
[33] Destatis: Zensus, URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Bevoelkerung/Bevoelkerungsstand/Tabellen/Zensus_Geschlecht_Staatsangehoerigkeit.html (aufgerufen am 18.08.2015).
[34] Vgl. Anlage 4.1, Personalausweisbroschüre S.16.
[35] Vgl. Anlage 4.1, Personalausweisbroschüre S.16.
[36] Personalausweisportal: Funktionen, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Funktionen/funktionen_node.html (aufgerufen am 18.08.2015).
[37] Vgl. Anlage 4.3, Email des BSI über Nutzungszahlen.

qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen.“

4.2 Rechtliche Rahmenbedingungen für die eID-Funktion

Bei der Umsetzung und Nutzung der eID-Funktion gibt es rechtliche Rahmenbedingungen, die einzuhalten sind, und dazu dienen einen bundesweit einheitlichen Standard zu schaffen. Die nachfolgend aufgeführten Rahmenbedingungen müssen bei der Anbietung der eID-Funktion eingehalten werden um eine gesetzeskonforme Nutzung des nPA zu gewährleisten[38]:

- Personalausweisgesetz (PAuswG)
- Personalausweisverordnung (PAuswV)
- Gesetz zur Förderung der elektronischen Verwaltung (EGovG)
- Verwaltungsverfahrensgesetze des Bundes und der Länder
- Leitlinie für die Vergabe von Berechtigungen an Dienstanbieter
- Technische Richtlinien des BSI

Außer den oben aufgeführten Rahmenbedingungen gilt es noch die eiDAS-VO zu beachten, welche ab 2016 für alle Mitgliedsstaaten der EU gilt. Im Allgemeinen regelt sie “ […] die europaweite Anerkennung elektronischer Identifizierungsmittel und die grenzüberschreitende Verwendung von elektronischen Signaturen, Zustelldiensten und weiterer sog. Vertrauensdienste […].“[39] In Punkt 14 der Verordnung wird festgelegt „ […] welche elektronischen Identifizierungsmittel anerkannt werden müssen und wie die elektronischen Identifizierungssysteme notifiziert werden sollten.“ Punkt 15 bestimmt für welche elektronischen Identifizierungsmittel eine Pflicht zur gegenseitigen Anerkennung besteht.

4.3 Voraussetzungen für die Nutzung

Um die eID-Funktion des nPA überhaupt nutzen zu können müssen bestimmte Voraussetzungen gegeben sein. Der Nutzer soll eine Gewährleistung haben, dass der Dienstanbieter berechtigt ist seine Daten

[38] Vgl. Anlage 4.4, Leitfaden Online-Ausweisfunktion in Behörden, S.8.
[39] Sosna, Sabine, S. 825.

zu nutzen. Im Gegenzug benötigt auch der Dienstanbieter eine Gewissheit, mit wem er es zu tun hat. Was sowohl Nutzer als auch Dienstanbieter zur Anwendung der eID-Funktion benötigen wird in den nachfolgenden Abschnitten erläutert.

4.3.1 Was benötigt der Nutzer?

In erster Linie muss die eID-Funktion eingeschaltet sein. Diese wird direkt bei Ausstellung des nPA auf der Behörde aktiviert oder kann nachträglich gegen eine erneute Gebühr aktiviert werden.[40] Zusätzlich wird eine 6-stellige PIN benötigt, welche nach der Beantragung des Ausweises per Brief zugestellt wird.[41] Sie wird als persönliches Passwort benötigt. Der Brief enthält außerdem eine PUK-Nummer, die dazu benötigt wird die eID-Funktion zu entsperren, beispielsweise wenn die PIN zu oft falsch eingegeben wurde.[42] Zudem erhält der Nutzer ein Sperrkennwort um den Ausweis sperren zu lassen wenn er abhandenkommt.[43]

Zur eingeschalteten eID-Funktion und der PIN werden außerdem ein geeignetes Kartenlesegerät und Software benötigt.[44] Es gibt Basislesegeräte, Standardlesegeräte und Komfortlesegeräte, die sich preislich und in ihrem Funktionsumfang unterscheiden.[45] Die Software hat eine Vermittlerrolle zwischen Nutzer und Dienstanbieter. Das BMI hat als

[40] Personalausweisportal: Beantragung, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Beantragung/beantragung_node.html (aufgerufen am 08.08.2015).

[41] Personalausweisportal: PIN-PUK-Sperrkennwort, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Pin-Puk-Sperrkennwort/Pin-Puk-Sperrkennwort-node.html (aufgerufen am 08.08.2015).

[42] Personalausweisportal: PIN-PUK-Sperrkennwort, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Pin-Puk-Sperrkennwort/Pin-Puk-Sperrkennwort-node.html (aufgerufen am 08.08.2015).

[43] Personalausweisportal: PIN-PUK-Sperrkennwort, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Pin-Puk-Sperrkennwort/Pin-Puk-Sperrkennwort-node.html (aufgerufen am 08.08.2015).

[44] Personalausweisportal: Das brauche ich, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/das-brauche-ich_node.html (aufgerufen am 08.08.2015).

[45] Personalausweisportal: Kartenlesegeräte, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Kartenlesegeraete/Kartenlesegeraete_node.html (aufgerufen am 08.08.2015).

Software ´AusweisApp2´[46] entwickelt. Die Online-Ausweisfunktion ist durch die benötigte Infrastruktur örtlich gebunden an die Stelle, wo Lesegerät und Software miteinander arbeiten können. Laut der Website der ´AusweisApp2´ soll die benötigte Software aber ab Ende 2015 auch für mobile Endgeräte zur Verfügung stehen.[47]

4.3.2 Was benötigt der Dienstanbieter?

Auch der Dienstanbieter benötigt eine gewisse Infrastruktur um für seine Dienste die Online-Identifikation anbieten zu können. Er muss festlegen, welche Datenfelder er vom nPA auslesen will und muss dafür ein Berechtigungszertifikat beantragen. Die Zulassung von Dienstanbietern erfolgt über die Vergabestelle für Berechtigungszertifikate beim Bundesverwaltungsamt.[48] Der Dienstanbieter benötigt zudem einen eID-Server, eine eID-Clientsoftware und ein Kartenlesegerät. Dieses Kartenlesegerät ist entweder das Gerät beim Nutzer oder ein in einen Automaten integriertes Kartenlesegerät.

Zertifikate werden überwiegend aus zwei Gründen erteilt.[49] Zum einen wenn aus einem gesetzlichen Grund die Nutzung der eID-Funktion benötigt wird, also beispielsweise eine Altersverifikation erfolgen soll, und zum anderen „ […] wenn ein erhebliches ´kreditorisches Risiko´ angenommen werden muss.“[50] Das ist beispielsweise dann der Fall, wenn ein Dienstleister teure Ware an einen Kunden schickt und dafür in Vorleistung tritt.[51] Um die Ware nicht an eine ungeprüfte Wohnanschrift zu senden erfolgt in diesen Fällen eine Wohnortbestätigung.

---

[46] Ausweisapp, URL: https://www.ausweisapp.bund.de/startseite/ (aufgerufen am 08.08.2015).
[47] Ausweisapp, URL: https://www.ausweisapp.bund.de/startseite/ (aufgerufen am 08.08.2015).
[48] Bundesverwaltungsamt: Vergabestelle, URL: http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_S/nPA/Vergabestelle/node.html (aufgerufen am 08.08.2015).
[49] Vgl. Imhof, Maximilian, S. 51.
[50] Borchers, Detlef, S. 139.
[51] Vgl. Borchers, Detlef, S. 139.

Die Schritte um Dienstanbieter zu werden sind auf nachfolgender Abbildung noch einmal dargestellt:

Abbildung 1: Dienstanbieter werden

Quelle: http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/diensteanbieter_node.html (aufgerufen am 26.08.2015)

4.4 Ablauf der Online-Identifikation mit dem nPA

Möchte ein Nutzer einen eID-Dienst nutzen muss er die Website des von ihm gewählten Dienstanbieters aufrufen und den gewünschten Dienst anfragen. Die Anfrage wird von der Website des Dienstanbieters an den eID-Server weitergeleitet. Dieser versucht eine Verbindung mit der Software und dadurch mit dem Lesegerät und dem auszulesenden nPA aufzubauen. Daraufhin werden die Authentizität von Nutzer und Dienstanbieter und die Integrität des Ausweises geprüft. Dem Nutzer wird angezeigt, welche Daten der Dienstanbieter vom Personalausweis auslesen möchte und er entscheidet eigenständig, ob er der Übertragung der angeforderten Daten zustimmt. Stimmt der Nutzer der Übertragung zu

wird er aufgefordert seine persönliche PIN einzugeben. Durch die Bestätigung mit der PIN werden die Ausweisdaten an den eID-Server übertragen. Dieser leitet die entsprechenden Ausweisdaten an den Dienstanbieter weiter. Der Nutzer erhält anschließend eine Benachrichtigung über die erfolgreiche Übertragung der Daten und der angeforderte Dienst wird ausgeführt.

Der Ablauf ist auf nachfolgender Abbildung nochmals dargestellt.

Abbildung 2: Ablauf der Online-Identifikation mit dem nPA

Quelle: Personalausweisportal: Online-Ausweisen, URL: http://www.personalausweisportal.de/DE/Wirtschaft/Technik/Online-Ausweisen/Online-Ausweisen_node.html (aufgerufen am 09.08.2015).

4.5 Vor- und Nachteile der eID-Funktion des nPA

Die eID-Funktion des nPA bringt viele Vorteile mit sich. Sie ermöglicht medienbruchfreie Abläufe und versichert dem Dienstanbieter die Qualität und Richtigkeit der Daten.[52] Es kann nicht mehr zur falschen Datenübernahme durch Lese- oder Tippfehler kommen.

[52] Personalausweisportal: Vorteile, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Vorteile/Vorteile_node.html (aufgerufen am 26.08.2015).

Im Bereich der öffentlichen Verwaltung bietet die eID-Funktion für Nutzer den großen Vorteil, dass sie nicht mehr persönlich auf dem Amt erscheinen müssen. Dadurch werden Zeit und Geld gespart.[53] Die ersparte Zeit kann in der Verwaltung für andere Dinge aufgewendet werden, wodurch Mitarbeiter der Verwaltung flexibler und abwechslungsreicher einsetzbar sind. In der heutigen Zeit wird es zudem immer wichtiger rund um die Uhr die Möglichkeit zu haben etwas zu erledigen. Viele Menschen leben in keinem klassischen Zeitmodell mehr. Deshalb kommt es vielen entgegen auch zu ungewöhnlichen Zeiten oder an Wochenenden und Feiertagen Anträge bei einer Behörde stellen zu können. Durch die Bindung an das Kartenlesegerät und einen Computer ist das System allerdings nicht so flexibel, wie es nötig wäre um den Nutzern eine tatsächliche Erleichterung zu bringen.

4.6 Mögliche Anwendungsbereiche und zugelassene Dienstanbieter

Auf der vom BMI unterstützten Webseite www.personalausweisportal.de[54] gibt es eine komplette Auflistung aller bisherigen Dienstanbieter in Deutschland. Auf Seiten der öffentlichen Verwaltung sind in vielen Behörden unter anderem bereits folgende Anwendungen möglich[55]:

- Wohnortbestätigung
- Beantragung von Führungszeugnissen
- Beantragung von Meldebescheinigungen
- Anträge auf Kindergeld
- Erklärungen zum Elterneinkommen
- KfZ-Zulassungen
- Anforderung von Briefwahlunterlagen, etc.

[53] Personalausweisportal: Vorteile, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Vorteile/Vorteile_node.html (aufgerufen am 26.08.2015).

[54] Für mehr Informationen siehe http://www.personalausweisportal.de/DE/Home/home_node.html

[55] Personalausweisportal: Anwendungsbeispiele Länder, URL: http://www.personalausweisportal.de/DE/Verwaltung/Anwendungsbeispiele/Laender/Laender_node.html (aufgerufen am 09.08.2015).

Zudem gibt es in den meisten Bundesländern die Möglichkeit der Online-Steuererklärung[56] und es gibt zahlreiche Vorhaben[57] die zukünftig weiter entwickelt und in Verwaltungsabläufe integriert werden sollen. Außerhalb der öffentlichen Verwaltung bieten bereits viele Versicherungen, Banken, die Deutsche Bahn und andere Unternehmen für einen Teil ihrer Dienstleistungen die eID-Funktion an. Der nPA bietet darüber hinaus noch weitere potenzielle Einsatzmöglichkeiten in Unternehmen und Behörden.[58]

4.7 Datenschutz- und Datensicherheit

Der nPA verfügt über eine ganze Liste von Sicherheitsmerkmalen, die Datenmissbrauch verhindern sollen. Insgesamt gibt es 23 Sicherheitsmerkmale beim neuen Personalausweis.[59] Die Daten des nPA können nur mit einem gültigen Berechtigungszertifikat und nur nach erfolgreicher Eingabe der PIN übertragen werden.[60] Ein ungewolltes Auslesen oder Übertragen von Daten ist somit ausgeschlossen und die Datensicherheit wird erhöht.[61] Die Übertragung von Daten erfolgt schrittweise und geschieht über „ international anerkannte und etablierte Verschlüsselungsverfahren“[62]. Die zwei wichtigsten Prinzipien für Datenschutz beim nPA sind:[63]

---

[56] Personalausweisportal: Anwendungsbeispiele Länder, URL: http://www.personalausweisportal.de/DE/Verwaltung/Anwendungsbeispiele/Laender/Laender_node.html (aufgerufen am 09.08.2015).

[57] Für mehr Informationen siehe: http://www.personalausweisportal.de.

[58] Personalausweisportal: Einsatzmöglichkeiten, URL: http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/Einsatzmoeglichkeiten/Einsatzmoeglichkeiten_node.html (aufgerufen am 25.08.2015).

[59] Vgl. Anlage 4.5, Flyer Bundesdruckerei Sicherheitsmerkmale.

[60] Personalausweisportal: Sicherheit und Datenschutz, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html (aufgerufen am 26.08.2015).

[61] Personalausweisportal: Sicherheit und Datenschutz, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html (aufgerufen am 26.08.2015).

[62] Bundesverwaltungsamt: Vergabestelle, URL: http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_S/nPA/Vergabestelle/ node.html (aufgerufen am 26.08.2015).

[63] Personalausweisportal: Sicherheit und Datenschutz, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html

- Das Prinzip der Datensicherheit

  Der Nutzer weiß immer, wem er seine Daten übermittelt und kann sicher sein kann, dass der von ihm gewählte Dienstanbieter berechtigt ist die Daten zu erhalten.

- Das Prinzip der Datensparsamkeit

  Bei der Übermittlung der Daten des Nutzers an den Dienstanbieter werden immer nur die Daten übermittelt, für die der Dienstanbieter laut seinem Zertifikat auch eine Berechtigung hat.

4.8 Probleme und Hindernisse bei der Nutzung

Trotz der vielen Sicherheitsmechanismen und der sichtbaren Sicherheitsmerkmale weist der nPA auch Lücken und Hindernisse auf. So kam es 2013 zur Aufdeckung einer Sicherheitslücke, durch die angeblich persönliche Daten abgegriffen werden konnten.[64] Ein Selbstläufer ist die eID-Funktion des nPA bislang nicht geworden, da die Motivation Geld für Kartenlesegeräte auszugeben sehr gering ist, solange für den nPA so wenige Möglichkeiten zur Nutzung bestehen. Die Nutzung am Computer ist zwar eine Vereinfachung im Vergleich zum Gang aufs Amt, jedoch hat sich die Nutzung von Online-Diensten in vielen Bereichen längst vom Computer auf das Smartphone oder Tablet verlagert. Das Problem ist, dass zwar eine elektronische Identifikation ermöglicht wird, das Ausweisdokument jedoch physisch vorliegen muss um es nutzen zu können.

Auch Dienstanbieter müssen Hürden überwinden bevor sie ein Berechtigungszertifikat erhalten. Zudem bedeutet das Anbieten der eID-Funktion auch einen Kostenfaktor, den sich nicht jedes Unternehmen leisten kann. Für Behörden stellen einige Länder zur Umgehung dieses

(aufgerufen am 26.08.2015).

[64] Stern Magazin: Sicherheitslücke nPA, URL: http://www.stern.de/panorama/chaos-computer-club-sicherheitsluecke-im-neuen-personalausweis-entdeckt-3908450.html (aufgerufen am 11.08.2015).

Problems bereits eID-Infrastrukturen zur Verfügung.[65] Das erfolgt immer öfter auch über Zweckverbände wie beispielsweise ´KIRU´[66] und ´DVV BW´[67] in Baden-Württemberg. So können Kosten gespart werden, der Aufwand bleibt überschaubar und das Berechtigungszertifikat kann von mehreren Behörden gemeinsam genutzt werden.[68]

[65] Vgl. Anlage 4.4, Leitfaden Online-Ausweisfunktion in Behörden S. 13.
[66] Für mehr Informationen siehe www.rz-kiru.de.
[67] Für mehr Informationen siehe www.dvv-bw.de.
[68] Vgl. Anlage 4.4, Leitfaden Online-Ausweisfunktion in Behörden S. 13-14.

5 Benutzung von Ausweisdokumenten in Neuseeland

In diesem Kapitel wird auf die Benutzung von Ausweisdokumenten in Neuseeland eingegangen. Zunächst werden allgemeine Informationen erläutert und anschließend geht es um rechtliche Grundlagen und um elektronische Ausweisdokumente in Neuseeland. Auch in diesem Kapitel soll der Fokus wieder auf die elektronische Identifikation gelegt werden.

5.1 Allgemeine Informationen und rechtliche Grundlagen

Anders als in Deutschland gibt es in Neuseeland keine gesetzliche Verpflichtung ein Ausweisdokument zu besitzen und daher kein einheitliches Ausweisdokument, das alle Neuseeländer besitzen.[69] Ausweisdokumente werden nur auf Antrag ausgestellt.[70]

Seitens des DIA wurde auf die Frage nach einer gesetzlichen Regelung zudem der Government Evidence of Identity Standard (EOI) als Leitfaden für Identitätsdokumente in Neuseeland genannt.[71] Eine weitere Auflistung ergibt sich aus dem ersten Teil des „ Amended Identity Verification Code of Practice 2013“ der Dienstanbieter verpflichtet die Identität ihrer Kunden bei bestimmten Transaktionen zu prüfen und es ist festlegt welche Identitätsdokumente dabei anerkannt werden können. Zudem spielt der Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT) eine Rolle da er vorschreibt, dass Dienstanbieter beim elektronischen Zahlungsverkehr ein Identitätsnachweis vom Auftraggeber der Zahlung verlangen müssen.

Aufgrund einer fehlenden abschließenden Regelung über in Neuseeland anzuerkennende Ausweisdokumente regelt jeder Dienstanbieter eigenverantwortlich welche Dokumente er als Identitätsnachweis anerkennt, hält sich dabei jedoch an den Amended Identity Verification Code of Practice 2013, den AML/CFT und den EOI Standard.

[69] Vgl. Anlage 5.1, Document Verification Guide, Foreword.
[70] Siehe Section 4, Passports Act 1992.
[71] Vgl. Anlage 5.2, E-Mail des Business Support Officer des DIA.

Neben dem neuseeländischen Reisepass, dem neuseeländischen Identitätszertifikat und der nationalen Identitätskarte können auch die Geburtsurkunde, der Führerschein, der Feuerwehrausweis oder die sogenannte 18plus-Karte zur Identifikation genutzt werden. Dies lässt sich dem Amended Identity Verification Code of Practice 2013 und den Identitätsanforderungen verschiedener Unternehmen und Banken entnehmen.

5.2 Elektronische Identifikation

Welche Regeln es in Bezug auf die elektronische Identifikation in Neuseeland gibt regelt der Electronic Identity Verification Act 2012. Ein elektronischer Identitätsnachweis enthält demnach mindestens die folgenden vier Daten[72]:

- Vorname und Nachname (full name)
- Geschlecht (gender)
- Geburtsdatum (date of birth)
- Geburtsort (place of birth)

Für jede Person kann maximal eine elektronische Identität bestehen.[73] Diese wird auf Antrag ausgestellt und es besteht, wie auch für die anderen Ausweisdokumente, keine Pflicht zum Besitz. In Neuseeland kann ab dem Alter von 14 Jahren eine elektronische Identität beantragt werden, wenn das Einverständnis eines Erziehungsberechtigten vorliegt.[74] Die Benutzung der elektronischen Identität ist im Electronic Identity Verification Act 2012 in den Abschnitten 16 bis 20 zu finden. In den Abschnitten 21 bis 25 ist geregelt, wer Zugang zu welchen elektronischen Daten hat. Der Electronic Identity Verification Act 2012 beschreibt keine bestimmte Form eines elektronischen Identitätsnachweises sondern stellt allgemeine Regelungen für die Erstellung und Benutzung von elektronischen Identitäten auf.

[72] Siehe Section 9, Electronic Identity Verification Act 2012.
[73] Siehe Section 11, Electronic Identity Verification Act 2012.
[74] Siehe Section 27, Electronic Identity Verification Act 2012.

Im März 2015 wurden in Neuseeland durchschnittlich bereits 48.5 % aller gezählten Dienstleistungen von Behörden online abgewickelt.[75] Das Ziel ist es, dass bis 2017 rund 70 % der häufigsten Geschäfte in Neuseeland online erledigt werden.[76] Zur Messung und damit zur Möglichkeit der Weiterentwicklung von Online-Diensten wurde das `Better Public Services Programme`[77] ins Leben gerufen. Dabei wird die Zunahme an Online-Aktivität im Bereich der 10 am häufigsten abgewickelten Geschäfte in Neuseeland gemessen. Result Nummer 10 ist das wichtigste Ziel, wenn es um die Messung von Online-Aktivität geht[78]: „New Zealanders can complete their transactions with government easily in a digital environment.“[79]

[75] RealMe: kiwis big users of online services, URL: https://www.realme.govt.nz/news/kiwis-big-users-online-services/ (aufgerufen am 11.08.2015).
[76] RealMe: kiwis big users of online services, URL: https://www.realme.govt.nz/news/kiwis-big-users-online-services/ (aufgerufen am 11.08.2015).
[77] State Services Commission: better public services, URL:http://www.ssc.govt.nz/better-public-services (aufgerufen am 11.08.2015).
[78] State Services Commission: interaction with government, URL: http://www.ssc.govt.nz/bps-interaction-with-govt#result10 (aufgerufen am 17.08.2015).
[79] Übersetzung: Neuseeländer können ihre Transaktionen mit der Regierung (öffentlichen Stellen) bequem in einem digitalen Umfeld abwickeln.

6 Das neuseeländische Konzept RealMe

In diesem Kapitel wird das neuseeländische Konzept RealMe zur elektronischen Identifizierung vorgestellt. Zunächst werden die Entstehung und Hintergründe von RealMe betrachtet. Danach erfolgt ein kurzer Überblick über die rechtlichen Rahmenbedingungen beim Betreiben der Dienste. Anschließend werden die unterschiedlichen Benutzerkonten vorgestellt. Es werden Vor- und Nachteile von RealMe gegenübergestellt und auch auf Datenschutz und RealMe für Dienstanbieter wird eingegangen.

6.1 Allgemeine Informationen

RealMe bietet eine einheitliche Anmeldung für Online-Dienste. Es wird vom Innenministerium in Zusammenarbeit mit der NZ Post zur Verfügung gestellt[80] und kann vom PC, Smartphone oder Tablet genutzt werden. Mit Hilfe von RealMe kann sich der Nutzer online gegenüber Behörden, Banken und Unternehmen ausweisen und zahlreiche Online-Dienste in Anspruch nehmen. Dadurch wird die Notwendigkeit der physischen Anwesenheit beim Erledigen behördlicher, und auch anderer Vorgänge, enorm reduziert. Das System basiert auf einer einzigartigen Kombination einer persönlichen Identitätsprüfung bei der NZ Post und einem Abgleich der Identitätsdaten mit Datenbanken durch das Department of Internal Affairs.[81] Es wurde erstellt um Online-Transaktionen in Neuseeland zu vereinfachen und die Notwendigkeit der physischen Anwesenheit zu reduzieren. Das Ziel war es das Verhältnis zu Behörden zu verbessern und den Menschen einen flexiblen, schnellen und einfachen Zugang zu Behörden und anderen öffentlichen Stellen wie Banken und Versicherungen zu ermöglichen.[82]

[80] RealMe: about us, URL: https://www.realme.govt.nz/about-us/ (aufgerufen am 26.08.2015).
[81] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).
[82] RealMe: power to people, URL: https://www.realme.govt.nz/news/power-people/(aufgerufen am 26.08.2015).

6.1.1 Entstehung und Hintergründe[83]

Der erste Online-Ausweisdienst in Neuseeland startete im April 2007 und war bekannt als ´Government Logon Service´. 2009 wurde die Zuständigkeit von der State Service Commission an das DIA abgegeben. Dadurch erfolgte eine Umbenennung in ´igovt´. 2011 wurde die NZ Post zuständig für die Vermarktung des Dienstes im privaten Sektor. Sie spielt bis heute eine entscheidende Rolle für den Online-Ausweisdienst. Im Juli 2013 wurde ´igovt´ schließlich von RealMe abgelöst. Nutzer des ehemaligen igovt-Dienstes konnten sich automatisch mit den bereits erfassten Daten ein RealMe-Benutzerkonto anlegen.

6.1.2 Rechtliche Rahmenbedingungen[84]

Der RealMe-Dienst muss sich an rechtliche Rahmenbedingungen halten. Dazu gehören auch allgemeine Web-Standards und Richtlinien. In nachfolgender Auflistung werden die wichtigsten Rahmenbedingungen aufgezählt.

- Electronic Identity Verification Act 2012
- Privacy Act 1993
- Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT)
- OASIS SAML 2.0 Standards und WS-Trust Standards
- NZ e-GIF Identity Management & Authentication Standards
- NZ Government Web Standards
- NZ Secure Web Services Standards
- NZ Security Manual
- Security in the Government Sector (SIGS)

[83] Vgl. Anlage 6.1, About RealMe, S. 1 RealMe design and development history.
[84] Vgl. Anlage 6.1 About RealMe, S. 1 RealMe meets strict design and operating requirements.

6.2 Die unterschiedlichen RealMe Benutzerkonten

Der RealMe Service bietet zwei unterschiedliche Arten von Benutzerkonten an, die sich im Wesentlichen dadurch unterscheiden, dass der Nutzer das eine Konto für den einheitlichen Login zu verschiedenen Online-Diensten nutzen kann. Beim anderen Benutzerkonto wird die Identität verifiziert, sodass mit diesem Konto online die Identität nachgewiesen werden kann. Nachfolgend werden beide Arten von Benutzerkonten, die Anforderungen und die möglichen Anwendungsbereiche vorgestellt. Darüber hinaus wird auch die Möglichkeit der verifizierten Adresse erläutert und die elektronische Signatur bei RealMe wird angesprochen.

6.2.1 Das nicht verifizierte RealMe Benutzerkonto

Das nicht verifizierte Benutzerkonto (RealMe Login) bietet einen zentralen Login um über 61 Onlinedienste von 20 öffentlichen Stellen nutzen zu können.[85] Zur Nutzung werden ein Benutzername und ein Passwort benötigt.[86]

Für die Registrierung benötigt der Nutzer eine E-Mail-Adresse, muss drei Sicherheitsfragen beantworten und den Nutzungsbedingungen zustimmen.[87] Alternativ zu den Sicherheitsfragen kann auch eine fünfstellige PIN verwendet werden die dann zum Tragen kommt, wenn das Passwort geändert werden soll.[88] Eine elektronische Identifikation ist mit diesem Benutzerkonto nicht möglich, jedoch erleichtert es den Nutzern den Zugang zu unterschiedlichen Online-Diensten, da der Nutzer sich nicht bei jeder Behörde getrennt anmelden muss. Der RealMe Login kann bei unterschiedlichen Stellen genutzt werden. Dazu gehören unter anderem die neuseeländische Unfallversicherung ACC, beinahe alle Ministerien, das Wählerverzeichnis, der Zoll, die Feuerwehr, die Polizei

[85] Vgl. Anlage 6.1, About RealMe, S. 1.
[86] RealMe: what it is, URL: https://www.realme.govt.nz/what-it-is/ (aufgerufen am 15.08.2015).
[87] Vgl. Anlage 6.1, About RealMe, S. 2, Process of getting a RealMe login.
[88] RealMe: PIN-numbers, URL: https://www.realme.govt.nz/help/#pin-numbers (aufgerufen am 15.08.2015).

und die New Zealand Transport Agency.[89] Zudem bietet der Login Zugang zu Stadt- und Bezirksverwaltungen. Dazu gehören bislang die Verwaltungen von Auckland, Hamilton, Rotorua, Wanganui und Wellington.[90] Dort können zum Beispiel Zahlungen vorgenommen werden, Anfragen gestellt werden, der Hund angemeldet werden und Änderungen der persönlichen Daten an die Behörde gemeldet werden. Es kommen laufend neue Anwendungsbereiche und Dienstanbieter hinzu.

6.2.2 Das verifizierte RealMe Benutzerkonto

Mit dem verifizierten RealMe-Konto können sich Nutzer in Echtzeit online gegenüber bestimmten Stellen ausweisen. Dabei wird zum bestehenden RealMe Login eine verifizierte Identität hinzugefügt.[91] Dadurch können online Transaktionen durchgeführt werden, die sonst nur durch ein persönliches Erscheinen durchführbar gewesen wären. Aktuell geht das gegenüber sechs sowohl öffentlichen als auch privaten Stellen. Über diese Art von Benutzerkonto können die im Electronic Identity Verification Act 2012 geforderten persönlichen Daten verbindlich nachgewiesen werden.

Zukünftig sollen noch weitere Informationen mit aufgenommen werden, die auch verbindlich nachweisbar sind.[92] Das verifizierte Benutzerkonto hat eine Gültigkeit von fünf Jahren.[93] Nach Ablauf dieser Zeit müssen die Identitätsnachweise erneut vorgelegt werden und ein neues Foto wird aufgenommen.[94]

---

[89] RealMe: where to use RealMe, URL: https://www.realme.govt.nz/what-it-is/where-to-use-realme/(aufgerufen am 12.08.2015).
[90] RealMe: where to use RealMe, URL: https://www.realme.govt.nz/what-it-is/where-to-use-realme/(aufgerufen am 12.08.2015).
[91] RealMe: what it is, URL: https://www.realme.govt.nz/what-it-is/ (aufgerufen am 12.08.2015).
[92] Vgl. Anlage 6.1, About RealMe, S. 1.
[93] RealMe: renewing your verified identity, URL:https://www.realme.govt.nz/help/# renewing-your-verified- identity (aufgerufen am 14.08.2015).
[94] RealMe: renewing your verified identity, URL:https://www.realme.govt.nz/help/# renewing-your-verified- identity (aufgerufen am 14.08.2015).

6.2.2.1 Verifizieren des Benutzerkontos[95]

Das Verifizieren des Benutzerkontos erfolgt in mehreren Schritten. Zuerst erfolgt eine normale Registrierung für den RealMe-Dienst, danach muss bei einer Geschäftsstelle der NZ Post noch ein Foto aufgenommen werden. Zusätzlich zu den für die Registrierung benötigten Daten muss eine Handynummer angegeben werden.[96] Diese wird zur sogenannten second-factor-authetication benutzt, welche in Kapitel 6.2.2.4 erklärt wird. Bei der Registrierung für ein verifiziertes Benutzerkonto muss der Nutzer die Daten eines der vier folgenden Dokumente eingeben[97]:

- Reisepass (Passport)
- Neuseeländische Geburtsurkunde (Birth)
- Einwanderungsnachweis (Immigration)
- Nachweis über Staatsbürgerschaft (Citizenship)

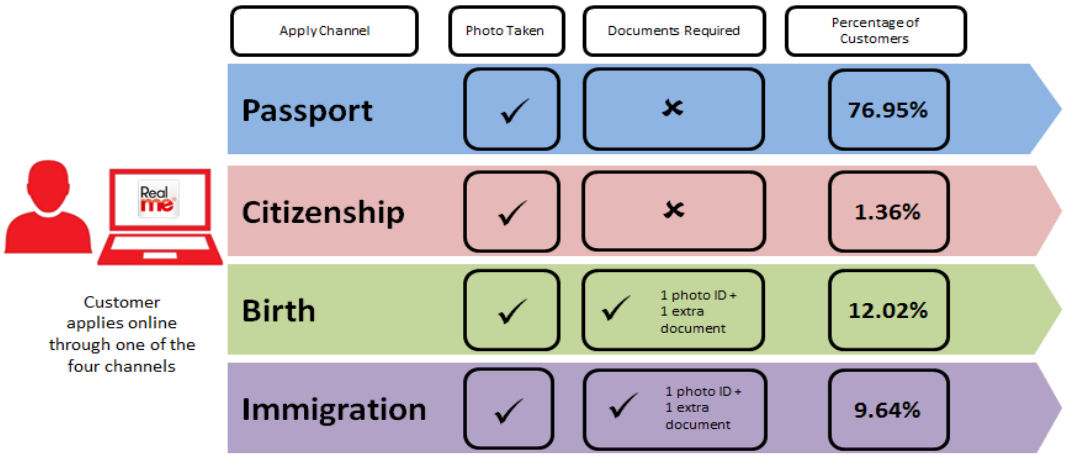
Danach erhält der Nutzer eine E-Mail mit einer einmaligen Referenznummer. Der nächste Schritt ist, dass der Nutzer innerhalb von 14 Tagen nach Beantragung der Verifikation mit der Referenznummer und einem der oben bereits aufgezählten Identitätsnachweise zur NZ Post geht. Besitzt der Nutzer einen Reisepass oder einen Nachweis über die neuseeländische Staatsbürgerschaft, der nach dem 01.01.2014 ausgestellt wurde, muss dieses Dokument nicht bei der NZ Post vorgelegt werden, da die Daten dann bereits elektronisch erfasst sind. Bei der Registrierung für ein verifiziertes Konto muss in diesen Fällen lediglich die Nummer des Dokuments eingegeben werden.[98]

Bei der NZ Post muss die Referenznummer vorgelegt werden und anschließend wird ein Foto des Nutzers aufgenommen. Das Foto und die vorgelegten Dokumente werden gescannt und an das DIA zur Überprüfung weitergeleitet. Das DIA gleicht das aufgenommene Foto

[95] Vgl. Anlage 6.1, About RealMe, S. 2-3 How RealMe works.
[96] RealMe: verify your identity, URL:https://www.realme.govt.nz/what-it-is/verify-your-identity/ (aufgerufen 14.08.2015).
[97] Vgl. Anlage 6.1, About RealMe, S. 2-3 How RealMe works.
[98] RealMe: documents you may need, URL: https://www.realme.govt.nz/what-it-is/verify-your-identity/documents-you-may-need/ (aufgerufen am 14.08.2015).

biometrisch mit anderen von der Person existierenden Fotos ab. Die eingereichten Dokumente werden ebenfalls mit bestehenden Datenbanken abgeglichen.[99] Bestehen alle Dokumente und das Foto die Überprüfung wird das verifizierte Benutzerkonto freigegeben und kann genutzt werden. Nachfolgende Abbildung zeigt, mit welchem Identitätsnachweis sich die meisten Nutzer bei der NZ Post ausweisen. In den meisten Fällen ist dies der Reisepass. Dies hat den Hintergrund, dass die Zielgruppe, die RealMe hauptsächlich anspricht, auch die Gruppe von Personen ist, die es zum Studieren, Arbeiten oder Reisen immer öfter in andere Länder zieht. Es handelt sich um Digital Natives, also die erste Generation von Personen die mit dem Internet aufgewachsen ist und auch um diejenigen, die das Internet als Bestandteil ihrer Arbeit oder Freizeit regelmäßig nutzen.

Abbildung 3: Benötigte Nachweise und Nutzungszahlen des verifizierten Benutzerkontos



Quelle: Anlage 6.1, About RealMe, S. 3, Figure 1.

6.2.2.2 Was benötigt der Nutzer?

Um die Online-Identifikation von RealMe nutzen zu können benötigt der Nutzer ein verifiziertes RealMe Benutzerkonto. Um dieses zu erstellen muss er sich zunächst mit einer gültigen E-Mail-Adresse bei RealMe registrieren und dann die in Kapitel 6.2.2.1 aufgezählten Schritte

[99] Vgl. Anlage 6.1, About RealMe, S. 3 How RealMe works.

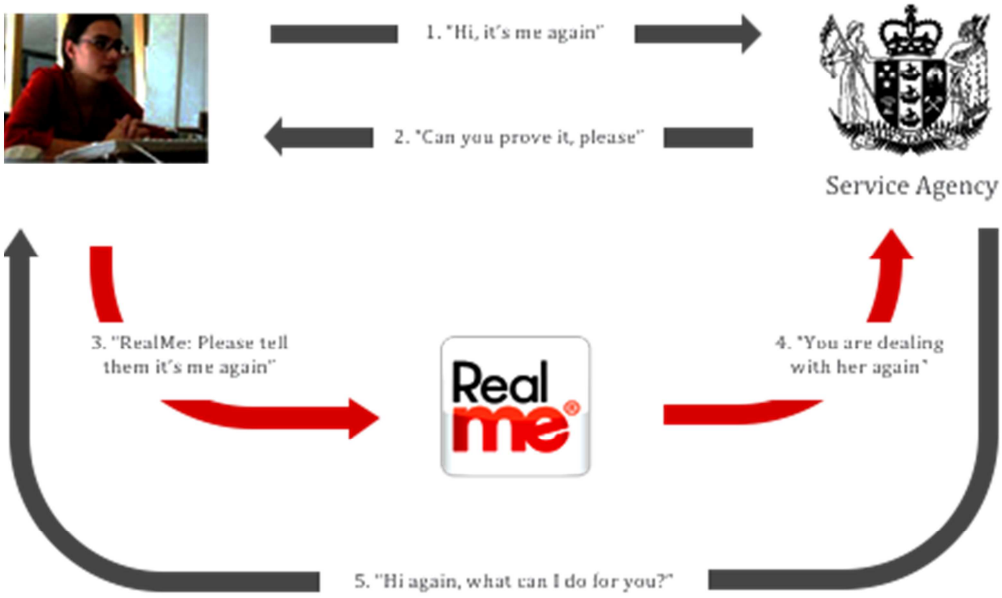
durchlaufen um sein Konto zu verifizieren. Zudem muss eine Mobiltelefonnummer hinterlegt werden, die dann bei der second-factor-authentication benötigt wird.

Je nach angefordertem Dienst können anstatt dem Mobiltelefon hierfür auch RealMe-Token verwendet werden.[100] Token sind Hardware-Geräte, die dem Nutzer bei Bedarf vom DIA zur Verfügung gestellt werden.[101]

6.2.2.3 Der Ablauf einer Online-Identifikation mit RealMe

Nachfolgende Abbildung stellt den Ablauf der Online-Identifikation mit RealMe vereinfacht dar. Die second-factor-authentication, die in Kapitel 6.2.2.4 erläutert wird, ist hier nicht veranschaulicht.

Abbildung 4: Ablauf der Online-Identifikation mit RealMe



Quelle: ICT: RealMe Login Service, URL: https://www.ict.govt.nz/services/show/RealMe-Login-Service (aufgerufen am 14.08.2015).

Zur Nutzung von RealMe als Online-Identifikationsnachweis geht der Nutzer auf die Seite des Dienstanbieters. Bietet dieser RealMe für eine Online-Identifikation an, meldet der Nutzer sich über den RealMe Login auf der Seite des Dienstanbieters bei seinem Benutzerkonto an. Der

[100] RealMe: tokens, URL: https://www.realme.govt.nz/help/#tokens (aufgerufen am 14.08.2015).
[101] RealMe: terms of use, URL: https://www.realme.govt.nz/terms-use/realme-terms-use/ (aufgerufen am 14.08.2015).

Nutzer bittet dann sozusagen RealMe dem Dienstanbieter seine Identität nachzuweisen. RealMe-Service bestätigt dem Dienstanbieter die Identität des Nutzers und der angeforderte Dienst wird für den Nutzer freigegeben bzw. durchgeführt. RealMe nimmt dabei lediglich eine Vermittlerrolle ein. Das angeforderte Ausweisdokument muss zu keinem Zeitpunkt physisch vorliegen, da alle Daten elektronisch abgerufen werden.

6.2.2.4 Second-Factor-Authentication

Um einen höheren Grad an Sicherheit zu erlangen wird für die Online-Identifikation mit RealMe die sogenannte „second-factor-authentication“, auf Deutsch Zwei-Faktoren-Authentifikation, angewendet.[102] Diese fragt beim Nutzer zwei Faktoren ab. Zum einen etwas, was er weiß (something you know), also den Benutzernamen und das Passwort, und zum anderen etwas, was er hat (something you have), beispielsweise ein Mobiltelefon.[103] Dadurch ist das Durchführen von Transaktionen online sicherer als nur durch Eingabe eines Benutzernamen und Passwort.[104]
Bei dieser Art von Authentifikation wird zur Ausführung des Dienstes ein weiteres Kennwort benötigt um mit Sicherheit zu wissen, dass der Nutzer auch derjenige ist, der er behauptet zu sein. Dieses zusätzliche Kennwort kann dem Nutzer auf verschiedenen Wegen übermittelt werden. Entweder über eine Textnachricht an das registrierte Mobiltelefon, über ein RealMe Token[105] oder über die App ´Google Authenticator´.[106] Bei allen drei Arten wird ein zusätzliches Kennwort aus einer zufällig generierten Zahl an den Nutzer gesendet. Erst nach Eingabe dieses Kennwortes kann sich der Nutzer gegenüber dem Dienstanbieter online identifizieren.[107] Dies dient sowohl dem Schutz des Nutzers, dessen Benutzerkonto und persönliche

[102] RealMe: second-factor-authentication, URL:https://www.realme.govt.nz/help/#second-factor-authentication (aufgerufen am 14.08.2015).
[103] RealMe: second-factor-authentication, URL: https://www.realme.govt.nz/help/#second-factor-authentication (aufgerufen am 14.08.2015).
[104] RealMe: second-factor-authentication, URL: https://www.realme.govt.nz/help/#second-factor-authentication (aufgerufen am 14.08.2015).
[105] RealMe: tokens, URL: https://www.realme.govt.nz/help/#tokens (aufgerufen am 14.08.2015).
[106] RealMe: second-factor-authentication, URL: https://www.realme.govt.nz/help/#second-factor-authentication (aufgerufen am 14.08.2015).
[107] RealMe: second-factor-authentication, URL: https://www.realme.govt.nz/help/#second-factor-authentication (aufgerufen am 14.08.2015).

Daten dadurch besser geschützt werden, als auch dem Dienstanbieter, der sich auf doppeltem Weg sicher sein kann, mit wem er es zu tun hat.

6.2.3 Die verifizierte Adresse[108]

Neben der Möglichkeit der elektronischen Identifikation bietet RealMe auch die Möglichkeit der verifizierten Adresse. Wenn der Nutzer beispielsweise ein neues Konto bei der Bank eröffnen möchte benötigt die Bank einen Nachweis über den Wohnsitz. Diese verifizierte Adresse ist zu vergleichen mit der Wohnortbestätigung beim nPA, allerdings wird beim nPA nur die Postleitzahl übermittelt. Bei RealMe geht es um eine Verifikation der kompletten Wohnanschrift.

Der Ablauf um die eine Adresse zu verifizieren ist wie folgt. Zunächst meldet der Nutzer sich bei seinem RealMe Benutzerkonto an und trägt dort seine neuseeländische Wohnanschrift ein. Daraufhin erhält er an diese Wohnanschrift einen Brief der NZ Post mit einem Kennwort. Dieses Kennwort muss er in seinem Benutzerkonto eingeben und die Adresse ist bestätigt. Wenn der Nutzer bereits ein Benutzerkonto bei der NZ Post besitzt kann er dieses auch mit dem RealMe Benutzerkonto verbinden und die bei der NZ Post hinterlegte Adresse wird automatisch übernommen.[109] Die verifizierte Adresse funktioniert nur für private Wohnanschriften und nicht für Postfächer oder dergleichen.[110]

6.2.4 Die elektronische Signatur bei RealMe

Durch die Kooperation mit dem Dienst `Secured Signing`[111] wurde zu den Diensten von RealMe auch die elektronische Signatur aufgenommen.[112] Sie ist erst seit August 2015 für RealMe Nutzer verfügbar. Offiziell wird sie noch nicht auf der Homepage angeboten, jedoch wurde sie in der Rubrik

[108] RealMe: verify your address, URL: https://www.realme.govt.nz/what-it-is/verify-your-address/ (aufgerufen am 15.08.2015).
[109] RealMe: address verification terms of use, URL: https://www.realme.govt.nz/terms-use/address-verification-service-terms-use/ (aufgerufen am 15.08.2015).
[110] RealMe: verify your address, URL: https://www.realme.govt.nz/what-it-is/verify-your-address/ (aufgerufen am 15.08.2015).
[111] Für mehr Informationen siehe: http://www.securedsigning.com/.
[112] RealMe: secured signing, URL: https://www.realme.govt.nz/news/secured-signing-joins-realme/ (aufgerufen am 17.08.2015).

´News` mehrfach vorgestellt.[113] `Secured Signing` ermöglicht es den Nutzern ihr Smartphone, Tablet oder ihren PC dafür zu nutzen Dokumente mit einer elektronischen Signatur zu versehen. Die Nutzung mit mobilen Endgeräten macht das ganze sehr flexibel und jederzeit für den Nutzer zugänglich.[114] In Kombination mit der verifizierten Identität bietet die elektronische Signatur dem Nutzer eine zuverlässige Möglichkeit die Echtheit einer Unterschrift gegenüber einem Dienstanbieter zu gewährleisten.[115]

6.2.5 Mögliche Anwendungsbereiche

Für Benutzerkonten mit verifizierten Identitäts- und Adressdaten gibt es zum jetzigen Stand sieben Dienstanbieter[116], doch die Zahl wird weiter steigen und es werden Dienstanbieter für die Nutzung der elektronischen Signatur hinzukommen. Von den sieben Dienstanbietern benötigen drei nur die verifizierte Identität ohne eine zusätzlich verifizierte Adresse, um Transaktionen durchführen zu können. Diese sind bislang das DIA, wo der Nutzer Geburts-, Todes-, und Heiratsurkunden, sowie Zertifikate über die eingetragene Lebenspartnerschaft beantragen kann.[117] Zudem die Electoral Commission, über die der Nutzer sich ins Wählerverzeichnis eintragen kann und dort auch Änderungen bei der eigenen Eintragung im Wählerverzeichnis vornehmen kann.[118] Der dritte Dienstanbieter, der nur eine verifizierte Identität verlangt ist Studylink. Dort besteht die Möglichkeit sich mit einem RealMe Benutzerkonto für einen Studienkredit und Fördermittel für das Studium zu bewerben.[119]

Bislang gibt es vier Dienstanbieter die sowohl eine verifizierte Adresse als auch eine verifizierte Identität fordern um Transaktionen durchführen zu

[113] RealMe: news, URL: https://www.realme.govt.nz/news/ (aufgerufen am 27.08.2015).
[114] RealMe: secured signing, URL: https://www.realme.govt.nz/news/secured-signing-joins-realme/ (aufgerufen am 17.08.2015).
[115] RealMe: secured signing, URL: https://www.realme.govt.nz/news/secured-signing-joins-realme/ (aufgerufen am 17.08.2015).
[116] RealMe: where to use RealMe, URL: https://www.realme.govt.nz/what-it-is/where-to-use-realme/ (aufgerufen am 15.08.2015).
[117] DIA: births, deaths, marriages, URL: http://www.dia.govt.nz/Births-deaths-and-marriages (aufgerufen am 15.08.2015).
[118] Electoral Commission, URL: http://www.elections.org.nz/ (aufgerufen am 15.08.2015).
[119] Studylink, URL: http://www.studylink.govt.nz/ (aufgerufen am 15.08.2015).

können.[120] Dabei handelt es sich um die drei Banken ´BNZ´[121], ´TSB´[122] und ´Westpac´[123], bei denen beide Arten von verifizierten Informationen benötigt werden um eine Konto eröffnen zu können. Außerdem gibt es noch ´NZ Forex´[124], bei denen ein Konto eröffnet werden kann um Überweisungen in ausländischen Währungen vorzunehmen. Zusätzlich können mit dem verifizierten Benutzerkonto auch die Dienstleistungen des RealMe Login, der in Kapitel 6.2.1 erklärt wurde, in Anspruch genommen werden.

6.3 RealMe für Dienstanbieter

RealMe versucht kontinuierlich die Liste seiner Dienstanbieter zu erweitern und neue Möglichkeiten zur Nutzung des RealMe Login und vor allem der verifizierten Identität und Adresse zu schaffen. Es bietet für Dienstanbieter eine bequeme und zuverlässige Möglichkeit zur Identifizierung ihrer Kunden. Es wird außerdem davon ausgegangen, dass durch die Möglichkeit Transaktionen online abzuwickeln mehr Kunden gewonnen werden und erhalten bleiben.[125] Das Anbieten der Identifikation über RealMe kostet den Dienstanbieter nur für diejenigen Kunden etwas, die dieses Angebot auch nutzen.[126] RealMe bietet in dieser Hinsicht eine größere Motivation für Unternehmen Dienstanbieter zu werden, da diese die Gewissheit haben, dass selbst wenn der Dienst nicht auslastend genutzt wird, die Kosten überschaubar bleiben.

Um RealMe als Dienst in ein Unternehmen zu integrieren muss das Unternehmen zunächst eine „participating agency“[127] nach den Auflagen

[120] RealMe: where to use RealMe, URL: https://www.realme.govt.nz/what-it-is/where-to-use-realme/ (aufgerufen am 15.08.2015).
[121] Für mehr Informationen siehe https://www.bnz.co.nz/.
[122] Für mehr Informationen siehe http://www.tsbbank.co.nz/.
[123] Für mehr Informationen siehe http://www.westpac.co.nz/.
[124] Für mehr Informationen siehe http://www.nzforex.co.nz/.
[125] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).
[126] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).
[127] Übersetzung: teilnehmendes Unternehmen.

der Electronic Identity Verification (EIV) Regulations 2013 sein. Das sind nach Abschnitt 4 der EIV Regulations 2013[128]:

- jede Organisation die nach Abschnitt 5 (1) des Public Audit Act 2011 eine öffentliche Stelle ist,
- alle Behörden des Parlaments (Office of Parliament) die unter den Abschnitt 2 (1) des Public Finance Act 1989 fallen, und
- alle registrierten Banken die unter den Abschnitt 2 (1) des Reserve Bank of New Zealand Act 1989 fallen.

Unternehmen die nicht hierzu gehören müssen sich an RealMe wenden und erfahren dann Unterstützung bei der Eintragung als `participating agency`.[129] Zusätzlich benötigt der Dienstanbieter eine passende Infrastruktur. Für diese technische Integration bieten sich zwei Lösungen an. Die erste wäre die Integration in die eigene, beim Dienstanbieter bestehende, Infrastruktur. Die Alternative ist die Nutzung des ´Cloud Identity Integrator´ der Firma Datacom.[130] Diese Alternative spart Zeit und Aufwand und stellt dem Dienstanbieter die benötigte Infrastruktur zur Verfügung. Zusätzlich zur Infrastruktur benötigt der Dienstanbieter Sicherheitszertifikate um zu gewährleisten, dass der angebotene Dienst keine Sicherheitslücken aufweist.[131]

6.4 Nutzung von RealMe im Vergleich zur physischen Identifikation

RealMe bietet sowohl seinen Nutzern als auch den Dienstanbietern Vorteile im Vergleich zur physischen Identifikation. Diese Vorteile und die Unterschiede zum nPA sollen in den nachfolgenden Abschnitten dargestellt werden.

[128] Siehe Section 4, Electronic Identity Verification Regulations 2013.
[129] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).
[130] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).
[131] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).

6.4.1 RealMe im Vergleich zum nPA

Der Unterschied von RealMe zum nPA besteht darin, dass bei der Nutzung von RealMe das eigentliche Ausweisdokument nicht physisch vorliegen muss. Dieses wird nur beim Verifizieren und gegebenenfalls Verlängern des Benutzerkontos benötigt. Zudem bestehen in Neuseeland ganz andere Anforderungen an Ausweisdokumente als in Deutschland.

Es ist grundsätzlich kein zusätzliches Gerät notwendig, außer der Nutzer verwendet RealMe Token für die second-factor-authentication.[132] Der Nutzer benötigt nur einen PC oder ein mobiles Endgerät um RealMe zu nutzen. Auch die Zwei-Faktoren-Authentifizierung erfolgt über eines dieser Geräte oder ein RealMe Token. RealMe ist dadurch kostengünstiger für den Nutzer und Dienstanbieter als der nPA, da diese nicht so viel Infrastruktur benötigen. Es ist für Unternehmen attraktiver Dienstanbieter zu werden als in Deutschland, da die Gegenüberstellung von Kosten und Nutzen für den Dienstanbieter in Neuseeland besser ausfällt. Dies wird dadurch begünstigt, dass beim Dienstanbieter, wie in Kapitel 6.3 dargestellt, eine kundengenaue Abrechnung der Kosten erfolgt.

Ein weiterer großer Unterschied ist, dass RealMe zusätzlich biometrische Daten zur Identifikation nutzt. „ […] Linking a RealMe applicant's photo to their biometric identity is what sets RealMe apart from its competitors[133]", so Mandy Smith, NZ Post Head of Agency Services.[134]

Es muss beachtet werden, dass es sich bei RealMe um ein komplett unterschiedliches System zur elektronischen Identifizierung handelt. In Neuseeland ist das Ausweisdokument an sich, mit Ausnahme der neuen Reisepässe[135], nicht elektronisch, während der nPA in Deutschland über den kontaktlosen Chip bereits über elektronisch abrufbare Daten verfügt.

---

[132] RealMe: terms of use, URL: https://www.realme.govt.nz/terms-use/realme-terms-use/ (aufgerufen am 14.08.2015).

[133] Übersetzung: Das Bewerbungsfoto des Nutzers mit seinen biometrischen Identitätsdaten zu verknüpfen ist das, was RealMe von seinen Konkurrenten unterscheidet.

[134] RealMe: biometric security, URL: https://www.realme.govt.nz/news/realme-brings-biometric-security-within-arms-reach/ (aufgerufen am 17.08.2015).

[135] Customs: epassports, URL: http://www.customs.govt.nz/features/smartgate/

6.4.2 Vorteile durch die Nutzung von RealMe

RealMe bietet im Allgemeinen die gleichen Vorteile wie der nPA in Deutschland. Durch den Abgleich der Identitätsdaten des Kunden mit den gespeicherten Datensätzen des DIA kann es kaum zu Identitätsmissbrauch kommen. RealMe erspart zudem das manuelle Erfassen von Daten und verhindert, wie auch die eID-Funktion des nPA, dass es zu Tippfehlern oder Auslassungen kommt. Der Nutzer hat eine ständige Kontrolle über seine Daten und entscheidet selbst ob und wann er diese mit Dienstanbietern teilt.[136] Er kann sich unabhängig von Ort und Zeit an diese wenden. Dadurch hat er die Möglichkeit auch vom Ausland aus Angelegenheiten in Neuseeland zu erledigen.[137] In Neuseeland bietet die Unabhängigkeit von Öffnungszeiten und bestimmten Orten deshalb einen Vorteil, da Menschen zum Teil in großen Entfernungen zu Städten, und somit auch zu Behörden und Dienstanbietern, leben. Der RealMe-Dienst ist flexibel einsetzbar und die dafür benötigte Infrastruktur ist bei einem Großteil der Nutzer bereits vorhanden, so dass hierfür in den meisten Fällen keine separaten Kosten anfallen. Der einzige Aufwand den der Nutzer hat, ist der einmalige Gang zur NZ Post.

6.4.3 Nutzungsauswertung anhand von Statistiken

In diesem Abschnitt werden aktuelle Zahlen zur Nutzung und Entwicklung von RealMe vorgestellt. Das soll dabei helfen einen Überblick zu erhalten, wie sich die Nutzung von RealMe seit der Einführung verändert hat, wie viele Benutzerkonten es derzeit in etwa gibt und wie viele Transaktionen bislang mit RealMe durchgeführt wurden. Abbildung 5 stellt dar, wie sich die Erstanmeldungen und die Nutzung des RealMe Login in den vergangenen Jahren entwickelt haben.

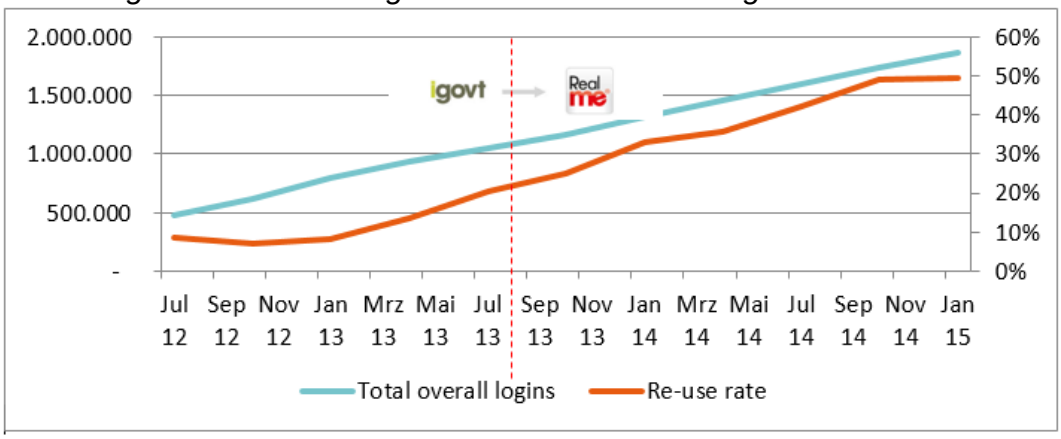
---

epassports/Pages/default.aspx (aufgerufen am 17.08.2015).

[136] RealMe: business, URL: https://www.realme.govt.nz/realme-business/ (aufgerufen am 17.08.2015).

[137] RealMe: life abroad, URL: https://www.realme.govt.nz/news/life-abroad-just-got-easier-thanks-realme/ (aufgerufen am 17.08.2015).

Abbildung 5: Erstanmeldungen und Wiederbenutzung



Quelle: Anlage 6.1, About RealMe, progress to date, figure 2.

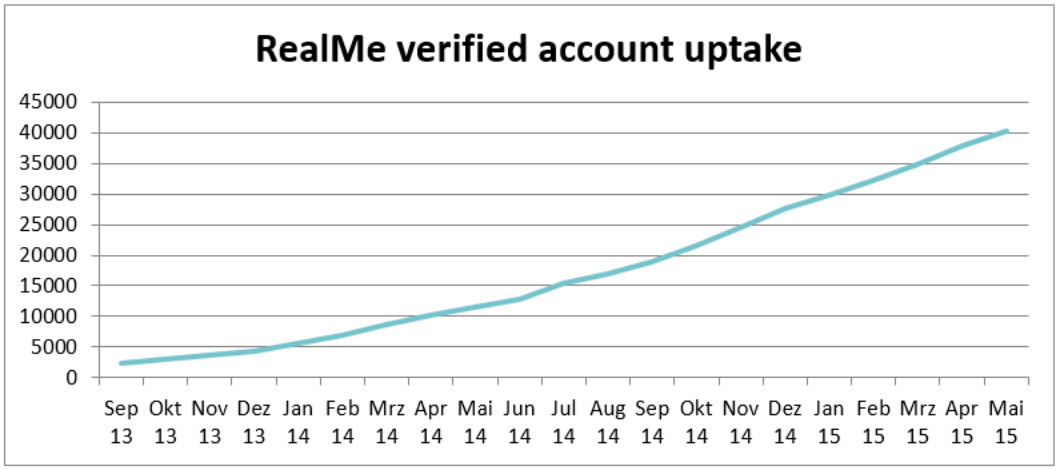
Bei den Anmeldungen (total overall logins) ist eine klare Tendenz nach oben zu erkennen. Die Wiederbenutzung (re-use rate) des RealMe Logins stagniert seit dem Spätjahr 2014 bei etwa 50% ist aber bis dahin stetig gewachsen.

Die Daten von ´igovt´ können deshalb mit einbezogen werden, da mit der Einführung von RealMe im Jahr 2013 zwar das verifizierte Benutzerkonto eingeführt wurde,[138] der RealMe Login aber identisch ist mit dem früheren igovt-Login und bestehende igovt-Benutzerkonten übernommen wurden.

Abbildung 6 zeigt die Entwicklung der verifizierten Benutzerkonten seit der Einführung im Jahr 2013. Die Abbildung zeigt einen kontinuierlichen Anstieg. Es ist davon auszugehen, dass diese Statistik zum aktuellen Stand einen weiteren Anstieg verzeichnet. Aktuellere Statistiken konnten von RealMe leider nicht zur Verfügung gestellt werden.

[138] RealMe: change log, URL: https://www.realme.govt.nz/changelog/ (aufgerufen am 27.08.2015).

Abbildung 6: Anstieg der verifizierten Benutzerkonten



Quelle: Anlage 6.1, About RealMe, verified identity uptake, figure 3.

RealMe ist sehr bestrebt seinen Nutzern und anderen Interessierten aktualisierte Zahlen zur Verfügung zu stellen. Auf der Homepage von RealMe werden täglich Nutzungszahlen aktualisiert. Zum aktuellen Stand[139] wurden seit der Einführung von RealMe insgesamt 2,11 Millionen RealMe Logins und 66 330 verifizierte Benutzerkonten angelegt, und 34.8 Millionen Transaktionen mit Hilfe des Dienstes durchgeführt. [140]

6.5 Datenschutz und Sicherheit[141]

RealMe speichert keine der personenbezogenen Daten, die der Nutzer benötigt um sich gegenüber Dienstanbietern auszuweisen. Es dient lediglich als Kanal zur Datenübermittlung. Bei RealMe werden nur die Daten abgespeichert, die zur Betreibung des Benutzerkontos benötigt werden, also Benutzername und Passwort. Der Nutzer entscheidet darüber, was für Daten er freigibt und kann über sein Benutzerkonto nachverfolgen welche Daten er mit wem geteilt hat. [142]

Einen weiteren Pluspunkt in Sachen Datenschutz und Sicherheit spielt die bereits erklärte second-factor-authentication. Ohne Eingabe des

[139] Datum: 07.09.2015.
[140] RealMe: about us, URL: https://www.realme.govt.nz/about-us/ (aufgerufen am 07.09.2015).
[141] RealMe: privacy and security, URL: https://www.realme.govt.nz/privacy-and-security/ (aufgerufen am 17.08.2015).
[142] RealMe: privacy and security, URL: https://www.realme.govt.nz/privacy-and-security/ (aufgerufen am 17.08.2015).

zusätzlichen Kennwortes können Transaktionen die einen höheren Grad an Sicherheit verlangen nicht durchgeführt werden.
Anhand der folgenden vier Punkte will RealMe dem Nutzer kontinuierlich Datenschutz und Sicherheit gewährleisten:

- RealMe berät sich regelmäßig mit dem Beauftragten für Datenschutz um sicherzustellen, dass Datenschutzanforderungen eingehalten werden.
- RealMe erhält jedes Mal Sicherheits-Folgenabschätzung, wenn an den Diensten von RealMe oder den zugrundeliegenden Regeln eine wesentliche Änderung vorgenommen wird.
- Auch für den Bereich des Datenschutzes werden bei Änderungen Folgeneinschätzungen vorgenommen. Bereits erfolgte Folgeneinschätzungen können online eingesehen werden.[143]
- Die Sicherheit der Dienste von RealMe wird laufend geprüft.

Um diese Punkte gewährleisten zu können arbeitet RealMe mit den Organisationen ´netsafe´[144] und ´ConnectSmart´[145] zusammen.

7 Ein mögliches RealMe-Konzept für Deutschland

Der nPA bietet grundsätzlich gute Ansätze bei der bundesweiten Ausgestaltung von E-Government und damit der Möglichkeit für den

[143] Für mehr Informationen siehe: https://www.realme.govt.nz/privacy-and-security/#privacy-impact-assessments.
[144] Für mehr Informationen siehe: https://www.netsafe.org.nz/.
[145] Für mehr Informationen siehe: https://www.connectsmart.govt.nz/.

Bürger einfacher und gezielter mit Behörden und auch anderen Dienstleistern zu agieren. Dass das bisherige System in Deutschland allerdings Lücken und Hindernisse aufzeigt wurde in Kapitel 4 dargestellt. In Kapitel 6 wurde das hervorragend funktionierende System RealMe aus Neuseeland vorgestellt, das sehr viel Zuspruch erhält und zunehmend an Nutzern gewinnt.

Um die Frage dieser Bachelorthesis beantworten zu können soll nun abgewogen werden, inwiefern ein System, ähnlich RealMe in Neuseeland, in Deutschland ein Ansatz für die Verwaltung sein könnte die bisherigen Möglichkeiten der Online-Identifizierung zu überdenken und ob dieses System implementierbar wäre. Der Fokus liegt dabei auf der Identifizierung gegenüber Behörden. Logischerweise wären bei einer möglichen Umsetzung auch andere Dienstanbieter inbegriffen.

In den nachfolgenden Abschnitten wird auf eine mögliche rechtliche, technische und organisatorische Umsetzung eingegangen. Anschließend werden Vor- und Nachteile eines solchen Konzeptes für Nutzer und Behörden abgewogen und Problemstellen aufgezeigt.

7.1 Rechtliche Umsetzung

Zur Implementierung eines solchen Systems bedarf es der Einhaltung von bestimmten rechtlichen Rahmenbedingungen. Für die elektronische Identifizierung in Deutschland existiert dieser rechtliche Rahmen bereits. Allerdings ist dieser Rahmen sehr genau auf die Nutzung mit dem nPA und eAT zugeschnitten und bildet daher möglicherweise ein Hindernis für die Implementierung anderer Systeme zur elektronischen Identifizierung in Deutschland.

7.1.1 Problematik durch rechtliche Rahmenbedingungen

Wie bereits erwähnt besteht für den nPA ein rechtlicher Rahmen, der die elektronische Benutzung des Personalausweises, die Vorgaben für Dienstanbieter sowie technische Richtlinien umfasst. Diese bereits existenten rechtlichen Rahmenbedingungen regeln die elektronische

Identifikation jedoch nicht allgemein, sondern nur in Bezug auf den nPA und zum Teil auch den eAT in Deutschland.

Das am 01.08.2013 in Kraft getretene E-Government-Gesetz (EGovG), dass zur Förderung der elektronischen Verwaltung beitragen soll, hat das Ziel „ […] die elektronische Kommunikation mit der Verwaltung zu erleichtern und Bund, Ländern und Kommunen zu ermöglichen, einfachere, nutzerfreundlichere und effizientere elektronische Verwaltungsdienste anzubieten.“[146] § 2 Absatz 3 EGovG verpflichtet die Behörden des Bundes dazu, dass Identitätsüberprüfungen zusätzlich zur regulären Identifikation durch Vorsprache auch durch einen elektronischen Identitätsnachweis nach § 18 PAuswG (nPA) oder § 78 Abs. 5 AufenthG (eAT) zu ermöglichen sind. Landesbehörden sowie Gemeinden oder Gemeindeverbände sind lediglich dazu verpflichtet zusätzlich zum postalischen Weg auch einen Zugang für die Übermittlung von elektronischen Dokumenten anzubieten.[147] Eine Pflicht zur Anbietung der elektronischen Identifikation besteht für sie nicht.

Sowohl § 18 Abs. 2 PAuswG als auch § 78 Abs. 5 AufenthG regeln, dass der elektronische Identitätsnachweis durch die Übermittlung der Daten aus dem elektronischen Speicher- und Verarbeitungsmedium des nPA bzw. eAT erfolgt. Identitätsdaten können also nach diesem Gesetz nur direkt vom jeweiligen elektronischen Ausweisdokument übertragen werden. Ein Hinterlegen der Daten, die dann bei Gebrauch abgerufen werden, so wie es bei RealMe gehandhabt wird, ist in Deutschland nicht erlaubt.

Zudem darf der RealMe-Dienst in Neuseeland auf biometrische Daten zugreifen. Dies ist in Deutschland für die elektronische Identifikation nicht vorgesehen.[148] Außerdem liegt ein Problem bei der Umsetzung des EGovG darin, dass es keine ausreichenden Regelungen für elektronische

[146] Bundesministerium des Innern: E-Government-Gesetz, URL: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Gesetz/e-government-gesetz_node.html (aufgerufen am 18.08.2015).
[147] Siehe § 2 Absatz 1 EGovG.
[148] Vgl. Anlage 7.1, Certificate Policy, Kapitel 1.1.

Identitäten trifft und durch Bundesrecht eingeschränkt werden kann.[149] Allgemein besteht eine große Rechtsunsicherheit in Fragen des E-Government, die es noch zu beseitigen gibt.[150] Zudem müssen weiterhin bundesrechtliche Hindernisse abgebaut werden, um die elektronische Kommunikation zwischen Bürger und Verwaltung noch einfacher zu gestalten.[151]

In Zeiten der Globalisierung und der Europäischen Union ist außerdem nicht jeder der in Deutschland lebt auch deutscher Staatsbürger und hat die Möglichkeit einen nPA zu besitzen oder besitzt aufgrund seines Aufenthaltes in Deutschland einen eAT. Daher wäre es für die Implementierung eines neuen Systems sinnvoll auch andere Ausweisdokumente zur elektronischen Identifizierung zuzulassen. Dadurch könnten auch Unionsbürger und Drittstaatenangehörige, die Verwaltungsdienste in Deutschland in Anspruch nehmen müssen, einbezogen werden. Durch ein Hinterlegen der Identitätsdaten würde an dieser Stelle auch keine Hürde durch die unterschiedlichen Ausweisdokumente, ob mit oder ohne Chip, entstehen.

Das EGovG regelt abschließend, wie Daten übertragen werden dürfen und das PAuswG sowie das AufenthG regeln, welche Daten übertragen werden dürfen. Die Gesetze lassen keinen Spielraum zu und sind exakt auf die bisherige deutsche Lösung zugeschnitten. Dadurch ist es derzeit rechtlich nicht möglich ein System wie RealMe in Deutschland zu implementieren. Eine Eins-zu-Eins-Umsetzung würde auch an der Übertragung biometrischer Daten scheitern. Eine Abwandlung des Systems oder eine Gesetzesänderung wären notwendig.

Trotz dieser Feststellung soll in den folgenden Abschnitten unter der Annahme, der rechtliche Rahmen würde entsprechend angepasst werden, herausgearbeitet werden, ob ein RealMe-ähnliches System in

[149] Siehe § 1 Abs. 4 EGovG.
[150] Vgl. Anlage 7.2, Minikommentar EGovG S.3.
[151] Vgl. Anlage 7.2, Minikommentar EGovG S.3.

Deutschland zur besseren Verbreitung und verstärkten Nutzung von elektronischen Identitäten dienen könnte.

7.2 Technische Umsetzung

Im Gegensatz zur rechtlichen Umsetzung wäre die technische Umsetzung relativ problemlos möglich. Für einen Dienst wie RealMe müssten lediglich eine Website mit einem Login und sichere Kanäle zum Abruf und zur Übertragung der Daten geschaffen werden. Berechtigungs- bzw. Sicherheitszertifikate für Dienstanbieter gibt es in beiden Systemen bislang auch schon.[152]

Der Nutzer wäre nicht mehr zwingend auf einen PC mit geeigneter Software und Lesegerät angewiesen, sondern würde nur noch sein Smartphone oder Tablet. Diese Geräte werden immer mehr genutzt[153] und würden für den Nutzer keinen zusätzlichen Aufwand darstellen.

Eine leicht abgewandelte Umsetzung könnte beispielsweise durch die Nutzung eines TAN-Generators erfolgen. Diese käme dem Prinzip bei RealMe gleich, Token zur Zwei-Faktoren-Authentifikation zu nutzen. Ein solches Prinzip, dass gleich dem Online-Banking bei vielen Banken ist, wäre vielen Menschen bereits bekannt und die Einarbeitung in ein neues System würde entfallen. Dadurch ist anzunehmen, dass ein solches, bereits bekanntes System schneller Nutzer finden würde. Allerdings würde der Nutzer ein zusätzliches Gerät, also den TAN- oder Token-Generator, mit sich führen müssen.

7.3 Organisatorische Umsetzung

Eine weitere spannende Frage ist, wie sich ein System wie RealMe in der deutschen Verwaltung organisatorisch umsetzen lassen könnte. Dass dies von sehr vielen verschiedenen Faktoren abhängt und wie unterschiedlich die Ausgangspositionen in Neuseeland und Deutschland sind wird nachfolgend dargestellt.

---

[152] Vgl. Kapitel 4.3.2 und 6.3.
[153] Vgl. Anlage 7.3, Mobile Fokusgruppe BVDW, S.4.

7.3.1 Zu beteiligende Institutionen

So wie in Neuseeland die Regierung mit der NZ Post zusammenarbeitet könnte auch in Deutschland die Regierung mit öffentlichen Stellen kooperieren. Wäre das Ganze abhängig von einer Beantragung bei der Gemeinde oder Stadt würde ein sehr großer Verwaltungsaufwand entstehen. Deshalb wäre es sinnvoll dem Nutzer mehrere unterschiedliche Anlaufstellen anzubieten.

Essentiell wäre es natürlich, dass seitens Bund, Ländern und Kommunen überhaupt eine Bereitschaft besteht ein neues System einzuführen und bisherige Anwendungen zu überdenken.[154]

Nach § 11 Abs. 3 EGovG müssten bei einer Änderung eines bestehenden Verfahrens eine Kontrolle nach dem Bundesdatenschutzgesetz durchgeführt werden und der Bundesbeauftragte für Datenschutz und Informationsfreiheit wäre anzuhören.

Zusätzlich sollte der IT-Planungsrat hinzugezogen werden um diese Zusammenarbeit zu steuern und unterstützend mitzuwirken.[155] Denn: „Durch die Einführung des Artikel 91c GG und die Schaffung des IT-Planungsrates wurden die Voraussetzungen für eine enge Zusammenarbeit von Bund und Ländern bei der Planung, der Errichtung und dem Betrieb ihrer informationstechnischen Infrastruktur erheblich verbessert.“[156] Der IT-Planungsrat könnte beratend wirken und es ist anzunehmen, dass er eine große Stütze bei der Umsetzung eines neuen Systems wäre.

Zudem wäre es sinnvoll einen Internetdienstanbieter, also einen Provider zu finden, der einheitlich die Server für Behörden bereitstellt und die Übermittlung von Daten vollzieht. Das BSI könnte dabei die Zulassung von Dienstanbietern steuern und die Einhaltung von Gesetzen und Richtlinien kontrollieren.

---

[154] Vgl. Anlage 7.2, Minikommentar EGovG S.3.
[155] IT-Planungsrat, URL: http://www.it-planungsrat.de/DE/Home/home_node.html (aufgerufen am 18.08.2015).
[156] Vgl. Anlage 7.2, Minikommentar EGovG S. 2.

7.3.2 Infrastruktur

Ein anderer wichtiger Punkt ist die Infrastruktur. Die erste Hürde stellt dabei die unterschiedliche Einwohnerzahl in Deutschland und Neuseeland dar. Neuseeland hat aktuell etwa 4,5 Millionen Einwohner[157], in Deutschland sind es um die 81 Millionen[158], also etwa 18-mal so viel.

Der Aufwand beim Verifizieren von Benutzerkonten wäre in Deutschland deutlich höher. Logischerweise steht in Deutschland auch eine breiter ausgebaute Infrastruktur zur Verfügung. Jedoch scheint es undenkbar, dass für jeden Bewerber eines verifizierten Kontos von einer einzigen Stelle ein Abgleich mit bestehenden Datenbanken durchgeführt wird. Das Konzept müsste in dieser Hinsicht abgewandelt werden und an die deutsche Verwaltung und Gesellschaft angepasst werden.

7.3.3 Voraussetzungen

Voraussetzung für eine optimal funktionierende Anwendung des elektronischen Identitätsnachweises wäre eine elektronische Aktenführung.[159] Dadurch könnten medienbruchfreie Abläufe geschaffen werden. „Voraussetzung ist allerdings, dass vor einer Digitalisierung die Prozesse analysiert und gegebenenfalls neu strukturiert werden und nicht lediglich eine elektronische Abbildung der Papierwelt stattfindet.“[160] Auch eine bessere Durchgängigkeit von E-Government in Bund, Ländern und Gemeinden wäre sehr hilfreich. So könnten bei Prozessen, an denen mehrere Behörden zu beteiligen sind auch mehrere gleichzeitig an einem Fall arbeiten, indem Akten elektronisch und somit auch vollständig und ohne die Gefahr es könnte etwas ausgelassen werden, übersendet werden. Das würde Bearbeitungs- und Wartezeiten zusätzlich verkürzen.

---

[157] Stats: national population estimates, URL: http://www.stats.govt.nz/browse_for_stats/population/estimates_and_projections/NationalPopulationEstimates_HOTPAt30Jun14.aspx (aufgerufen am 18.08.2015).

[158] Destatis: Zensus, URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Bevoelkerung/ Bevoelkerungsstand/Tabellen/Zensus_Geschlecht_Staatsangehoerigkeit.html (aufgerufen am 18.08.2015).

[159] Vgl. Mirbach, Dagmar, S. 38.

[160] Vgl. Anlage 7.2 Minikommentar EGovG S. 2.

Zudem wäre eine bessere Breitbandversorgung vor allem im ländlichen Raum notwendig, um einen solchen Dienst überhaupt sinnvoll und effizient einsetzen zu können. Anderenfalls werden Bewohner dieser Gegenden weiterhin durch persönliche Vorsprache ihre Angelegenheiten mit Behörden vornehmen.

Die Möglichkeit persönlich bei der Behörde vorzusprechen muss aber generell erhalten bleiben. Es kann nicht davon ausgegangen werden, dass jeder die Möglichkeit der elektronischen Identifizierung auch nutzen will und kann.

7.3.4 Möglichkeiten zu Förderung von Online-Diensten

Eine Möglichkeit zu Förderung von Online-Diensten in Deutschland wäre eine Art ´Better Public Services Programme´[161] für die deutsche Verwaltung. Also eine Art Aktionsplan mit festgelegten Zielen und Zeiträumen um Online-Dienste messbar und nachvollziehbar darstellen und auf dieser Grundlage weiterentwickeln zu können. Ein solcher Aktionsplan könnte, wenn nicht auf Bundes-, dann zumindest auf Landesebene schneller zu sichtbaren Erfolgen führen und Behörden motivieren.

Das bereits existierende Regierungsprogramm „ Digitale Verwaltung 2020“[162] setzt Ziele für eine Verwaltung der Zukunft und könnte als Ansatz zur Förderung von digitalen Prozessen in der Verwaltung betrachtet werden. Im Gegensatz zum ´Better Public Services Programme´ in Neuseeland ist es aber viel detaillierter ausgestaltet und wirkt dadurch schwerer greifbar. Ein einfach strukturierter Aktionsplan ohne eine zu genaue Beschreibung von möglichen Vorgehensweisen wäre jedoch wesentlich hilfreicher. Einzelne Behörden müssen die Gelegenheit haben einen Zugang zu den Vorhaben zu finden. Ein auf den Tisch gelegtes Regierungsprogramm sorgt weder für eine einheitliche Umsetzung noch

[161] Siehe Kapitel 5.2.

[162] Bundesministerium des Innern: Digitale Verwaltung 2020, URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/regierungsprogramm-digitale-verwaltung-2020.html (aufgerufen am 27.08.2015).

motiviert es dazu Strukturen neu zu schaffen. Den Behörden würde es vermutlich einfacher fallen schrittweise Änderungen zu vollziehen, anstatt einen großen Katalog mit Vorhaben und Zielen vorgelegt zu bekommen. In den Behörden selbst sind meistens einzelne Personen oder kleine Personenkreise für den Bereich IKT zuständig. Diese fühlen sich mit zu ausschweifenden Programmen schnell überfordert.

EU-weit gibt es bereits den „E-Government Aktionsplan der Europäischen Union“[163], jedoch ist dieser ein paar Ebenen zu hoch angesetzt um bei Landesverwaltungen, sowie Gemeinden und Städten im ausreichenden Maß umgesetzt zu werden. Es fehlt zudem an Kontrollmöglichkeiten. Die Idee eines EU-weit übergreifenden Systems und Ausbau von E-Government und Dienstleistungen ist berechtigt, jedoch kaum umsetzbar. Die einzelnen EU-Mitgliedsstaaten sind zu unterschiedlich in puncto Gesetzeslage, Infrastruktur und Verwaltungsaufbau um ohne großartige Veränderungen und Kostenaufwand ein einheitliches System einzuführen.

Auch das Projekt ´STORK´ der Europäischen Union bietet einen interessanten Ansatz zur Förderung von Online-Diensten, insbesondere auch der Online-Identifikation.[164] Auch bei ´STORK´ werden keine Daten abgespeichert.[165] Trotzdem scheitert eine erfolgreiche Umsetzung an den unterschiedlichen Rechtslagen in den Mitgliedsstaaten, da viele Staaten zwar bereits eigene Lösungen zur Online-Identifikation anbieten, diese aber nicht interoperabel sind und daher nur länderspezifisch genutzt werden können.[166]

Es gilt also zu entscheiden, ob man sich zunächst auf die Umsetzung einer deutschen Lösung konzentriert oder angesichts der immer weiterreichenden Vernetzung in Europa nicht direkt an einer übergreifenden europäischen Lösung arbeitet. Dabei gäbe es die Vor- und

[163] Europa: E-Government Aktionsplan, URL: http://ec.europa.eu/digital-agenda/european-egovernment-action-plan-2011-2015 (aufgerufen am 27.08.2015).
[164] Stork, URL: https://www.eid-stork.eu/ (aufgerufen am 27.08.2015).
[165] Stork: Erklärung, URL: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=186 (aufgerufen am 27.08.2015).
[166] Stork: Erklärung, URL: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=186 (aufgerufen am 27.08.2015).

Nachteile, die rechtliche Ausgangslage und auch die Kosten abzuwägen. Insbesondere die Annahme, dass sich ein EU-weites System in den Mitgliedsstaaten sehr unterschiedlich entwickeln würde und am Ende aller Wahrscheinlichkeit nach eine eher partielle Umsetzung und Nutzung herauskommen würde, schreckt vor dieser Alternative bisher ab.

In Anbetracht der geografischen Lage von Deutschland und seiner Zugehörigkeit zur EU wäre es dennoch sinnvoll schon jetzt über eine übergreifende Lösung nachzudenken. Neuseeland hat als Inselstaat den Vorteil, dass es nur mit wenigen anderen Systemen kooperieren muss und es sich von seiner geografischen Lage her eher eine isolierte Lösung leisten kann, die wenig Rücksicht auf andere Staaten nimmt.

Die Verwaltung muss sich auf jeden Fall bemühen ihre Dienstleistungen vermehrt in ein elektronisches Umfeld zu übertragen, „ […] um überhaupt in der dialogorientierten Online-Welt mithalten zu können.“[167]

7.4 Vor- und Nachteile beim Anbieten eines solchen Dienstes

Die Vorteile bei der Anbietung eines solchen Dienstes bestehen darin, dass sowohl für die Nutzer als auch die Dienstanbieter, also in diesem Fall vorzugsweise Behörden, die Kommunikation und der Umgang miteinander deutlich einfacher und unkomplizierter werden.

Der Nutzer erspart sich lange Warte- und Bearbeitungszeiten sowie Fahrtwege. Er ist nicht mehr so stark an die sachliche und örtliche Zuständigkeit von Behörden gebunden[168] und es können „ […] nutzerfreundliche, ebenenübergreifende Verwaltungsdienstleistungen auf einer gemeinsamen Oberfläche […]“[169] angeboten werden. „ Sie [Bürger] erwarten, dass Dienstleistungen der öffentlichen Verwaltung über die Grenzen der jeweiligen Stadt oder Gemeinde verfügbar sind.“[170] Von der Unabhängigkeit von bestimmten Orten zur Nutzung profitiert allerdings auch die Verwaltung, insbesondere die einzelnen Mitarbeiter, da flexiblere

[167] Habbel, Franz-Reinhard, S.453.
[168] Vgl. Anlage 7.2, Minikommentar EGovG S. 2.
[169] Vgl. Anlage 7.2, Minikommentar EGovG S. 2.
[170] Kehle, Roger, S. 28.

Arbeitszeiten und neue Arbeitsmodelle ermöglicht werden, was wiederum die Vereinbarkeit von Familie und Beruf fördert.[171] Ein solches System könnte wesentlich zur Verwaltungsmodernisierung und zum Bürokratieabbau beitragen.[172]

Die Nutzung über Smartphone oder Tablet bietet einen enormen Zuwachs an Flexibilität im Bereich der Kommunikation mit der Verwaltung. Gerade die Generation der Digital Natives trägt fast immer ein mobiles Endgerät bei sich und nutzt dieses. Durch die Möglichkeit der Nutzung eines RealMe-ähnlichen Dienstes sowohl mit mobilen Endgeräten als auch am PC hat der Nutzer überall einen Zugang zum Dienst und kann sich dabei sogar entscheiden, welches Gerät er für die Durchführung von Transaktionen nutzen möchte. Allerdings gehen Smartphones und Tablet wesentlich schneller verloren oder werden gestohlen als ein PC. Durch die Zwei-Faktoren-Authentifikation stellt dies allerdings keine größere Sicherheitslücke dar. Die Benutzung von PIN-Nummern und Kennwörtern bietet dem Nutzer eine große Sicherheit.

7.5 Problematik

Eine der größten Hürden ist außer den rechtlichen Rahmenbedingungen das bestehende System des nPA, der teuer eingeführt wurde. Trotz der eher schlechten Nutzungszahlen wird dieses bisherige System nicht ohne weiteres verworfen werden um mit einem grundlegend anderen Ansatz neu zu starten. Seitens der Regierung wird nicht zugegeben, dass die Einführung des nPA keine großen Erfolge mit sich gebracht hat. Ohne die Regierung als Unterstützung ist ein neues System, dass im Bereich der Verwaltung eingesetzt werden soll aber nicht umsetzbar.

Selbst wenn also die Grundlagen dafür geschaffen würden um ein System wie RealMe in Deutschland implementieren zu können, würde das bestehende System zur Online-Identifizierung, der nPA, den Weg versperren. Der Gedanke mit zwei unterschiedlichen Systemen gleichzeitig zu arbeiten ist zu verwerfen. Dies würde für Nutzer und

[171] Vgl. Anlage 7.2, Minikommentar EGovG S. 2.
[172] Vgl. Kehle, Roger, S. 28.

Dienstanbieter zu komplex und aufwendig werden, und keine Interoperabilität zulassen.

Zudem müssten angesichts der Bevölkerungszahl und somit potenziellen Benutzerzahl eine sehr große Menge personenbezogener Daten irgendwo auf einem Server abgespeichert werden um diese dann bei Bedarf abrufen zu können. Ein automatisiertes Abrufverfahren wäre nach § 10 BDSG zwar zulässig und auch die Übertragung personenbezogener Daten an öffentliche[173] und nicht-öffentliche[174] Stellen wäre zulässig. Die Speicherung von so enormen Datenmengen steht jedoch dem Prinzip der Datenvermeidung und Datensparsamkeit aus § 3a BDSG entgegen.

[173] Siehe § 15 BDSG.
[174] Siehe § 16 BDSG.

8 Mögliche Weiterentwicklung der Thematik

Die Chancen stehen gut, dass die elektronische Identifikation in Deutschland sich in den kommenden Jahren verändern und weiterentwickeln wird. Mit zunehmender Präsenz der Thematik werden sich immer mehr Behörden, Bürger und Fachleute mit den Möglichkeiten die sich bieten beschäftigen.

Durch veränderte oder verbesserte Nutzungsmöglichkeiten der Online-Identifikation wird auch die Zahl der Nutzer steigen. Das Angebot an Diensten bestimmt die Nachfrage. Umso attraktiver und vielfältiger das Angebot an Diensten sein wird, umso höhere Nutzungszahlen werden verzeichnet werden.

Egal ob das bestehende System weiter ausbaut oder ein neues System eingeführt wird, müsste dieses erneut und vermehrt beworben werden um potenzielle Nutzer auf die möglichen Einsatzgebiete aufmerksam zu machen. Es müssten sich mehr Dienstanbieter finden um ein breiteres Spektrum an Dienstleistungen für die Online-Identifikation nutzbar zu machen und dadurch auch eine breitere Zielgruppe anzusprechen. Die junge Generation, welche die elektronischen Möglichkeiten hauptsächlich nutzt, muss sich in den angebotenen Diensten wiederfinden können. Darauf sollte bei der Überlegung, welche Dienste angeboten werden, geachtet werden.

Langfristig könnte ein Wegfall von Arbeitsplätzen durch die zunehmende Digitalisierung befürchtet werden, jedoch bieten sich durch neue Systeme auch immer neue Einsatzmöglichkeiten und Herausforderungen, die es zu bewältigen gibt. Es ist wahrscheinlich, dass Arbeitsplätze aus Gründen der Digitalisierung abgeschafft werden, da sie überflüssig werden, jedoch können durch die neuen Anforderungen auch Arbeitsplätze mit neuartigen Aufgabenspektren geschaffen werden. Der Bürokratieaufwand wird von der Papierakte in elektronische Akte verlagert wodurch Ressourcen eingespart werden können. Klassische Öffnungszeiten können abgeschafft werden und es können neue Arbeitszeitmodelle entstehen.

Wichtig ist es, dass die bisherigen Möglichkeiten der Kommunikation mit Behörden trotzdem erhalten bleiben. Dies muss nicht mehr in dem Umfang geschehen, dass durchgehend alle Mitarbeiter einer Behörde als Ansprechpartner anwesend sind, es sollte aber bestimmte Öffnungszeiten geben, zu denen die Bürger ganz klassisch bei der Behörde vorsprechen kann. Dies kommt vor allem den Leuten entgegen, die das Internet nicht, oder nicht in einem großen Umfang nutzen, beispielsweise Senioren.

Der demographische Wandel bringt viele Herausforderungen mit sich, die durch den Einsatz elektronischer Verwaltungsdienste besser bewältigt werden können.[175] Voraussetzung ist, dass Problemstellen erkannt werden und herausgearbeitet wird, wie diese durch den Einsatz von E-Government beseitigt werden können. Angesichts der aktuellen Flüchtlingsproblematik in Deutschland wäre es auch sinnvoll zu überlegen den Weg der elektronischen Verwaltung, nicht nur in Hinsicht auf die Identifikation, auch für diese Menschen zu eröffnen um Verfahren zu beschleunigen und zu vereinfachen.

[175] Vgl. Anlage 8.1, Minikommentar EGovG, S.2.

9 Fazit

Die Beantwortung der Frage dieser Bachelorthesis, ob das neuseeländische Konzept RealMe zur elektronischen Identifizierung ein möglicher Ansatz für die deutsche Verwaltung ist, fällt nicht leicht.

Auf der einen Seite ist klar, dass der vermehrte Einsatz von elektronischen Prozessen in den Verwaltungsablauf auf Seiten von Nutzern und Behörden Erleichterungen mit sich bringt und viele Potenziale in dieser Hinsicht noch nicht ausgeschöpft werden.

Auf der anderen Seite wurde in dieser Bachelorthesis auch dargestellt, wo die Probleme bei der Implementierung eines Konzeptes wie RealMe in Deutschland liegen, und dass einige Hürden im Weg stehen.

Das Konzept RealMe ist nicht der optimale Ansatz für die deutsche Verwaltung. Die Unterschiede der beiden Länder in Bezug auf geografische Lage, Verwaltungsaufbau, Bevölkerungszahl und rechtliche Rahmenbedingungen sind zu groß um einen Eins-zu-Eins-Umsetzung erfolgreich durchzuführen. Trotzdem war die Ausarbeitung der Frage in dieser Bachelorthesis wichtig um festzustellen, dass es in Deutschland einer Änderung bedarf, wenn das Verwaltungshandeln tatsächlich weitgehend digitalisiert werden soll und für Bürger attraktiv gestaltet werden soll.

Es ist eindeutig zu erkennen, dass die bisherige Lösung in Deutschland nicht geeignet ist, um die elektronische Identifikation in dem Maß zu nutzen und in bestehende Abläufe integrieren zu können, dass sie eine Verbesserung und Vereinfachung von Behördengängen darstellt. Die Vorstellung des Konzepts RealMe hat deutlich gemacht wieviel Bürokratie sich durch einen gezielten und durchdachten Einsatz von E-Government vermeiden lässt und wie die Verwaltung für Bürger attraktiver und zugänglicher gestaltet werden kann.

Langfristig wird die Entscheidung ausstehen, ob die bisherige Lösung mit dem nPA beibehalten wird und eventuell weiter ausbaut wird, ob ein völlig

neues System implementiert werden soll, oder ob auf eine EU-weite Lösung spekuliert werden kann.

Die Handlungsempfehlung des Autors ist zum jetzigen Zeitpunkt zu versuchen, das System der eID mit dem nPA noch attraktiver zu gestalten und sich andere Länder, wie Neuseeland oder auch Estland und Österreich, als Vorbild in Sachen elektronische Identifikation zu nehmen um das System schrittweise zu verbessern. Es sollte überlegt werden, wie der nPA anders genutzt oder integriert werden kann, ohne den Ausweis an sich zu ändern. Eine Abschaffung des nPA als elektronisches Ausweisdokument wäre derzeit nicht sehr zielführend. Trotzdem muss an der Flexibilität und Interoperabilität des Systems weiter gearbeitet werden.

Zusammenfassend kann gesagt werden, dass es im Bereich der elektronischen Identifikation vielfältige Umsetzungsmöglichkeiten gibt, die an rechtliche und gesellschaftliche Gegebenheiten anzupassen sind um zufriedenstellende Nutzungszahlen zu erhalten. Auch wenn ein Konzept wie RealMe nicht die optimale Lösung für die deutsche Verwaltung darstellt gilt es am Ball zu bleiben. Es lohnt sich die Entwicklungen in diesem Bereich im Auge zu behalten um hoffentlich eines Tages persönlich erleben zu können, wie viele Vorteile der richtige Einsatz elektronischer Möglichkeiten uns bringen kann.

Literaturverzeichnis

Ausweisapp: URL: https://www.ausweisapp.bund.de/startseite/, aufgerufen am 08.08.2015.

Borchers, Detlef: Digitale Identität: Anwendungsszenarien für den elektronischen Personalausweis, in : c´t – Magazin für Computertechnik, 2010, Heft 23, S. 138-141.

Bundesamt für Sicherheit in der Informationstechnik: Elektronische Ausweise,
URL: https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/elektronischeausweise_node.html, aufgerufen am 08.08.2015.

Bundesministerium des Innern: Digitale Verwaltung 2020,
URL:http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/regierungsprogramm-digitale-verwaltung-2020.html, aufgerufen am 27.08.2015.

Bundesministerium des Innern: E-Government-Gesetz,
URL: http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/E-Government/E-Government-Gesetz/e-government-gesetz_node.html, aufgerufen am 18.08.2015.

Bundesministerium des Innern: elektronischer Reiseausweis,
URL: http://www.bmi.bund.de/DE/Themen/Moderne-Verwaltung/Ausweise-Paesse/Dokumente-Auslaender/Elektronischer-Reiseausweis/elektronischer-reiseausweis_node.html, aufgerufen am 25.08.2015.

Bundesverwaltungsamt: Vergabestelle,
URL: http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_S/nPA/Vergabestelle/node.html, aufgerufen am 08.08.2015.

Cole, Tim: Die digitale Identität macht alle zu Gewinnern,
in: Schwarz, Torsten (Hrsg.): Leitfaden Online-Marketing, 2008, S. 521-526, ISBN: 3-00-020904-2.

Customs: epassports,
URL: http://www.customs.govt.nz/features/smartgate/epassports/Pages/default.aspx, aufgerufen am 17.08.2015.

Destatis: Zensus,
URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Bevoelkerung/Bevoelkerungsstand/Tabellen/Zensus_Geschlecht_Staatsangehoerigkeit.html, aufgerufen am 18.08.2015.

DIA: births, deaths, marriages,
URL: http://www.dia.govt.nz/Births-deaths-and-marriages, aufgerufen am 15.08.2015.

Duden: Implementierung,
URL: http://www.duden.de/rechtschreibung/implementieren,
aufgerufen am 31.08.2015.

Duden: Interoperabilität,
URL: http://www.duden.de/rechtschreibung/Interoperabilitaet,
aufgerufen am 31.08.2015.

Duden: verifizieren,
URL: http://www.duden.de/rechtschreibung/verifizieren, aufgerufen am 07.09.2015.

Electoral Commission: URL: http://www.elections.org.nz/, aufgerufen am 15.08.2015.

Europa: E-Government Aktionsplan,
URL: http://ec.europa.eu/digital-agenda/european-egovernment-action-plan-2011-2015, aufgerufen am 27.08.2015.

Gabler Wirtschaftslexikon: E-Government,
URL: http://wirtschaftslexikon.gabler.de/Definition/electronic-government.html?referenceKeywordName=E-Government,
aufgerufen am 28.08.2015.

Habbel, Franz-Reinhard: Auf dem Weg zu Kommune 2.0,
in: Alcatel-Lucent Stiftung für Kommunikationsforschung, Gemeindetag Baden-Württemberg, Innenministerium Baden-Württemberg und Stiftung der Württembergische Gemeinde-Versicherung a.G. (Hrsg.): Praxis des E-Government in Baden-Württemberg, 2010, S. 449-454, ISBN: 978-3-415-04504-0.

ICT: RealMe Login Service,
URL: https://www.ict.govt.nz/services/show/RealMe-Login-Service,
aufgerufen am 14.08.2015.

Imhof, Maximilian: Der neue, elektronische Personalausweis,
Technische Universität München, Seminar Future Internet SS2011, Seminararbeit, 2011, S. 48-54.
Online verfügbar unter: http://www.net.in.tum.de/fileadmin/TUM/NET/NET-2011-07-2/NET-2011-07-2_07.pdf, aufgerufen am 08.08.2015.

IT-Planungsrat: URL: http://www.it-planungsrat.de/DE/Home/home_node.html, aufgerufen am 18.08.2015.

Kehle, Roger: Chancen des E-Government für baden-württembergische Gemeinden, in: Alcatel-Lucent Stiftung für Kommunikationsforschung, Gemeindetag Baden-Württemberg, Innenministerium Baden-Württemberg und Stiftung der Württembergische Gemeinde-Versicherung a.G. (Hrsg.): Praxis des E-Government in Baden-Württemberg, 2010, S. 28-30, ISBN: 978-3-415-04504-0.

Mirbach, Dagmar: Kommunale Verwaltung auf dem Weg in die digitale Zukunft, in: Innovative Verwaltung, Ausgabe 6/2015, S. 38-41.

Personalausweisportal: Anwendungsbeispiele Länder, URL: http://www.personalausweisportal.de/DE/Verwaltung/Anwendungsbeispiele/Laender/Laender_node.html, aufgerufen am 09.08.2015.

Personalausweisportal: Beantragung, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Beantragung/beantragung_node.html, aufgerufen am 08.08.2015.

Personalausweisportal: Das brauche ich, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/das-brauche-ich_node.html, aufgerufen am 08.08.2015.

Personalausweisportal: Der Ausweis mit dem Klick, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/der-personalausweis_node.html, aufgerufen am 08.08.2015.

Personalausweisportal: Dienstanbieter, URL: http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/diensteanbieter_node.html, aufgerufen am 08.08.2015.

Personalausweisportal: Einsatzmöglichkeiten, URL: http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/Einsatzmoeglichkeiten/Einsatzmoeglichkeiten_node.html, aufgerufen am 25.08.2015.

Personalausweisportal: FAQ Dienstanbieter, URL: http://www.personalausweisportal.de/DE/Wirtschaft/Diensteanbieter-werden/FAQ/faq_node.html#faq3241822, aufgerufen am 08.08.2015.

Personalausweisportal: Funktionen, URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Funktionen/funktionen_node.html, aufgerufen am 18.08.2015.

Personalausweisportal: Kartenlesegeräte,
URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Kartenlesegeraete/Kartenlesegeraete_node.html, aufgerufen am 08.08.2015.

Personalausweisportal: Online Ausweisen,
URL: http://www.personalausweisportal.de/DE/Wirtschaft/Technik/Online-Ausweisen/Online-Ausweisen_node.html, aufgerufen am 09.08.2015.

Personalausweisportal: PIN-PUK-Sperrkennwort,
URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Das-brauche-ich/Pin-Puk-Sperrkennwort/Pin-Puk-Sperrkennwort-node.html, aufgerufen am 08.08.2015.

Personalausweisportal: Sicherheit und Datenschutz,
URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Sicherheit-und-Datenschutz/Sicherheit-und-Datenschutz-node.html, aufgerufen am 26.08.2015.

Personalausweisportal: Vorteile,
URL: http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/Vorteile/Vorteile_node.html, aufgerufen am 26.08.2015.

RealMe: about us,
URL: https://www.realme.govt.nz/about-us/, aufgerufen am 26.08.2015 und am 07.09.2015.

RealMe: address verification terms of use,
URL: https://www.realme.govt.nz/terms-use/address-verification-service-terms-use/, aufgerufen am 15.08.2015.

RealMe: biometric security,
URL: https://www.realme.govt.nz/news/realme-brings-biometric-security-within-arms-reach/, aufgerufen am 17.08.2015.

RealMe: business,
URL: https://www.realme.govt.nz/realme-business/, aufgerufen am 17.08.2015.

RealMe: change log,
URL: https://www.realme.govt.nz/changelog/, aufgerufen am 27.08.2015.

RealMe: documents you may need,
URL: https://www.realme.govt.nz/what-it-is/verify-your-identity/documents-you-may-need/, aufgerufen am 14.08.2015.

RealMe: kiwis big users of online services,
URL: https://www.realme.govt.nz/news/kiwis-big-users-online-services/, aufgerufen am 11.08.2015.

RealMe: life abroad,
URL: https://www.realme.govt.nz/news/life-abroad-just-got-easier-thanks-realme/, aufgerufen am 17.08.2015.

RealMe: news,
URL: https://www.realme.govt.nz/news/, aufgerufen am 27.08.2015.

RealMe: PIN-numbers,
URL: https://www.realme.govt.nz/help/#pin-numbers, aufgerufen am 15.08.2015.

RealMe: power to people,
URL: https://www.realme.govt.nz/news/power-people/, aufgerufen am 26.08.2015.

RealMe: privacy and security,
URL: https://www.realme.govt.nz/privacy-and-security/, aufgerufen am 17.08.2015.

RealMe: renewing your verified identity,
URL: https://www.realme.govt.nz/help/#renewing-your-verified-identity, aufgerufen am 14.08.2015.

RealMe: second-factor-authentication,
URL: https://www.realme.govt.nz/help/#second-factor-authentication, aufgerufen am 14.08.2015.

RealMe: secured signing,
URL: https://www.realme.govt.nz/news/secured-signing-joins-realme/, aufgerufen am 17.08.2015.

RealMe: terms of use,
URL: https://www.realme.govt.nz/terms-use/realme-terms-use/, aufgerufen am 14.08.2015.

RealMe: tokens,
URL: https://www.realme.govt.nz/help/#tokens, aufgerufen am 14.08.2015.

RealMe: verify your address,
URL: https://www.realme.govt.nz/what-it-is/verify-your-address/, aufgerufen am 15.08.2015.

RealMe: verify your identity,
URL: https://www.realme.govt.nz/what-it-is/verify-your-identity/, aufgerufen am 14.08.2015.

RealMe: what it is,
URL: https://www.realme.govt.nz/what-it-is/, aufgerufen am 12.08.2015 und am 15.08.2015.

RealMe: where to use RealMe,
URL: https://www.realme.govt.nz/what-it-is/where-to-use-realme/, aufgerufen am 12.08.2015 und am 15.08.2015.

Sosna, Sabine: EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten- eiDAS-Verordnung, in: Computer und Recht, Ausgabe 12/2014, S. 825-832. ISSN: 0179-1990.

State Services Commission: better public services,
URL: http://www.ssc.govt.nz/better-public-services, aufgerufen am 11.08.2015.

State Services Commission: interaction with government,
URL: http://www.ssc.govt.nz/bps-interaction-with-govt#result10, aufgerufen am 17.08.2015.

Stats: national population estimates,
URL: http://www.stats.govt.nz/browse_for_stats/population/estimates_and_projections/NationalPopulationEstimates_HOTPAt30Jun14.aspx, aufgerufen am 18.08.2015.

Stern Magazin: Sicherheitslücke im neuen Personalausweis entdeckt, vom 27.08.2013, URL: http://www.stern.de/panorama/chaos-computer-club-sicherheitsluecke-im-neuen-personalausweis-entdeckt-3908450.html, aufgerufen am 11.08.2015.

Stingl, Johannes: E-Government-Strategie zur Erfüllung kommunaler Aufgaben, in: Alcatel-Lucent Stiftung für Kommunikationsforschung, Gemeindetag Baden-Württemberg, Innenministerium Baden-Württemberg und Stiftung der Württembergische Gemeinde-Versicherung a.G. (Hrsg.): Praxis des E-Government in Baden-Württemberg, 2010, S. 121-127, ISBN: 978-3-415-04504-0.

Stork: URL: https://www.eid-stork.eu/, aufgerufen am 27.08.2015.

Stork: Erklärung,
URL: https://www.eid-stork.eu/index.php?option=com_content&task=view&id=186, aufgerufen am 27.08.2015.

Studylink: URL: http://www.studylink.govt.nz/, aufgerufen am 15.08.2015.

Eidesstattliche Erklärung

Erklärung

„Ich versichere, dass ich diese Bachelorarbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet.

Es ist mir bekannt, dass die Arbeit mit einer Plagiaterkennungssoftware auf nicht gekennzeichnete Übernahme fremden geistigen Eigentums überprüft werden kann.“

Datum, Unterschrift